ETHICAL ISSUES IN A NETWORKED ENVIRONMENT

THESIS

Kristen G. Sallberg, Captain, USAF

AFIT/GIR/LAS/97D-11

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY
AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

AFIT/GIR/LAS/97D-11

ETHICAL ISSUES IN A NETWORKED ENVIRONMENT

THESIS

Kristen G. Sallberg, Captain, USAF

AFIT/GIR/LAS/97D-11

Approved for public release; distribution unlimited

The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

AFIT/GIR/LAS/97D-11

ETHICAL ISSUES IN A NETWORKED ENVIRONMENT

THESIS

Presented to the Faculty of the Graduate School of

Logistics and Acquisition Management of the

Air Force Institute of Technology

Air University

Air Education and Training Command

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Information Resource Management

Kristen G. Sallberg, B.A.

Captain, USAF

December 1997

Approved for public release; distribution unlimited

Acknowledgments

An AFIT experience is one which is unparalleled in the course of any career. My experience is one in which I am truly indebted to several individuals. I am especially grateful to my advisor, Dr. Alan Heminger, for his professional and personal support during this time. It can truly be said that I would not have finished this program without it. My thanks also goes to my reader, Dr. David Vaughan, for his considerable patience in reviewing innumerable drafts. His guidance regarding this research was invaluable. Mrs. Nancy Wiviott also has my appreciation for her professional assistance but also my thanks for her incredible patience with my consistent tardiness regarding deadlines.

My family has earned this degree right along with me. The help and support of my parents and grandmother with the care of my children during this difficult trek enabled me to actually accomplish my work while maintaining some semblance of sanity. My beautiful butterfly, Elisabeth, was incredibly patient for a four-year old while consistently reminding me of what is truly important. Her innocent reminders of "Mom, it's time you got your head out of your books!" and "Mommy, did you finish your homework so you can spend time with me?" could always bring a smile regardless of the time crunch I was under. She was truly a treasure during this time. I owe my adorable angel, Melissa, thanks for allowing me an uneventful first nine months with her so I could concentrate on my work and not morning sickness. She helped out in her own way by being such an incredibly happy baby and sleeping through the night within her first few weeks.

Finally, to my husband Scott, my thanks for his patience while attempting to coach me through the math phase of my coursework and putting up with me taking my frustrations out on him. Most importantly, for his love and care of our children during this time—especially his coverage of the 2- and 4-am feedings for Melissa. All I can say is *more than words.*

Kristen Gray Sallberg

Table of Contents

Page

Acknowledgments ii

List of Tables vii

Abstract x

I. Statement of Problem 1

Introduction 1
An Ethical Quandary 2
Why Should the USAF Be Concerned With This Ethical Quandary? 4
Importance of Issue 6
Problem Statement 9
Summary 11

II. Literature Review 13

Introduction 13
Networking Implications for the Military 14
Military Members and Network Usage 19
Unique Features of Network Technology 20
The Special Scope of Networked Systems 21
Anonymity in Networked Systems 23
Autonomy in a Networked Environment 27
Barriers to Accountability in a Networked Environment 30
Reproducibility in a Networked Environment 32
A Final Word on Unique Characteristics 33
Ethical Issues Regarding Network Usage 35
Privacy 36
Accuracy 40
Property 42
Accessibility 44
Computer Abuse and Misuse 45
Organizational Perspectives 46
The Military Perspective 47
USAF Network Specific Directives 51
AFI 33-119 Electronic Mail (E-Mail) Management and Use 1 Mar 97 51
AFI 33-129 Transmission of Information via the Internet 1 Jan 97. 54
Conclusion. 56

Page

III. Methodology 57

Introduction 57
Data Collection Method 58
Population and Sample Size 59
Data Analysis 60

IV. Survey Responses and Analysis 61

Introduction 61
Part I. Responses to Background Demographics 61
Question 1 61
Question 2 62
Question 3 63
Question 4 63
Question 5 64
Question 6 65
Question 7 65
Question 8 66
Part II. Responses to Network Related Data Questions 67
Question 9 67
Question 10 68
Question 11 69
Question 12 70
Question 13 70
Question 14 71
Question 15 71
Question 16 72
Part III. Sample Scenarios 73
Scenario 1 73
Scenario 2 75
Scenario 3 78
Scenario 4 80
Scenario 5 82
Scenario 6 84
Scenario 7 87
Scenario 8 91
A Concurrence of Views 95
Grade Consistencies 95
Age Consistencies 96
Level of Command Consistencies 98

Page

V. Conclusions and Recommendations 101

Introduction 101
Discussion 101
The Specific Research Objective 103
Limitations of Current Study 104
Recommendations for Future Research 104
A Final Word: Implications for USAF Managers 105

Appendix A: Survey 107

Appendix B: Difference between the Means Responses for Grade Groups 121

Appendix C: Difference between the Means Responses for Different Age Groups . . 122

Appendix D: Difference between Responses for Different Levels of Command 123

Bibliography 124

Vita 130

List of Tables

Table Page

1. What is your grade? 62

2. What is your age group? 63

3. How long have you been employed by the USAF? 63

4. How long have you been working in your present office? 64

5. At what level of command is your office located? 65

6. Do you directly supervise employees? 65

7. If you do not directly supervise employees are you considered a manager? 66

8. Do you consider yourself a computer user or computer professional? 67

9. Approximately how long has your office had access to a network? 68

10. What do you use your network access for? 69

11. In your present position, how often do you use your office network? 70

12. Do you use the network to accomplish: 70

13. Rate effectiveness of networking in enhancing your duty performance 71

14. Has your organization provided guidance regarding appropriate usage of organizational computer networks? 71

15. Have you ever observed inappropriate usage in the workplace? 72

16. Scenario 1: Question 1a 74

17. Scenario 1: Question 1b 74

18. Scenario 1: Question 1c 75

19. Scenario 1: Question 1d 75

Table Page

20. Scenario 2: Question 2a 76

21. Scenario 2: Question 2b 77

22. Scenario 2: Question 2c 77

23. Scenario 2: Question 2d 78

24. Scenario 3: Question 3a 79

25. Scenario 3: Question 3b 79

26. Scenario 3: Question 3c 80

27. Scenario 3: Question 3d 80

28. Scenario 4: Question 4a 81

29. Scenario 4: Question 4b 81

30. Scenario 4: Question 4c 82

31. Scenario 5: Question 5a 83

32. Scenario 5: Question 5b 83

33. Scenario 5: Question 5c 84

34. Scenario 5: Question 5d 84

35. Scenario 6: Question 6a 86

36. Scenario 6: Question 6b 86

37. Scenario 6: Question 6c 87

38. Scenario 6: Question 6d 87

39. Scenario 7: Question 7a 89

40. Scenario 7: Question 7b 90

41. Scenario 7: Question 7c 90

Table Page

42. Scenario 7: Question 7d 91

43. Scenario 7: Qúestion 7e 91

44. Scenario 8: Question 8a 93

45. Scenario 8: Question 8b 93

46. Scenario 8: Question 8c 94

47. Scenario 8: Question 8d 94

AFIT/GIR/LAS/97D-11

Abstract

The objective of this research was to provide a preliminary understanding of how United States Air Force computer users perceive the ethical considerations of computer networks and how the Air Force is addressing the ethical issues of a networked environment. To provide this understanding a survey was undertaken to explore questions of ethics in the use of information networks. The literature review for this study explored issues of ethics in the professional information systems environment and Air Force guidance regarding the usage of official government computer resources. The literature review provided a baseline for comparison of survey responses from the users.

The sample population of the study consisted of military members stationed at Wright-Patterson Air Force Base Ohio. The study found that responses regarding certain attitudes about behaviors and actions in a networked environment were consistent overall. Thirty-two questions addressing eight networking scenarios were presented to survey participants. A significant difference was observed between seven responses that addressed the issues of information privacy, unauthorized access, use of government software in the home, and personal use of government networks. However, although statistically significant, the differences were small. Regardless of grade, age or level of command, respondents generally responded in a similar manner to different situations. The findings suggest that Air Force members are aware of ethical considerations in the use of networked computers. The results of the research also

indicate that Air Force management is attuned with the professional information systems community pertaining to the guidance provided to Air Force members.

ETHICAL ISSUES IN A NETWORKED ENVIRONMENT

I. Statement of Problem

Introduction

Since its inception, the United States Air Force (USAF) has operated in a global environment. Whether in the form of flying operations or diplomatic support, the USAF has had a presence on virtually every continent since 1947. In recent years, however, the concept of global environment has changed dramatically. In addition to a tangible, physical global presence, the USAF must now grapple with an intangible global environment made possible by rapid advances in information technology (Schwartau, 1996:637). This intangible environment—often referred to as Cyberspace or the Global Network—is a result of the rapid expansion in computing capacity in conjunction with the proliferation of high-performance data communications networks (Schwartau, 1996:36). Day-to-day functions that used to be performed manually by humans have in many cases been computerized, either as a stand-alone system or an integrated network. These advances have enabled the service to streamline operations and provide organizations and employees access to a broader information base than previously available.

Although many of these recently developed tools have provided new capabilities, they have also introduced numerous unresolved issues and problems. A primary issue of interest to the USAF concerns the development of appropriate ethics policies and standards for the use of these new tools. The emergence of networks in the workplace has created possibilities for individual and institutional behavior that were not previously available (Johnson, 1994:3). Increased dependence on information systems and data communication networks presents managers and their staffs with new scenarios where traditional ethical issues acquire complex new twists (Forester and Morrison, 1995:10). The implications of a networked environment must be addressed by the USAF to maintain a duty atmosphere supporting the core values of integrity first, service before self, and excellence in all we do.

An Ethical Quandary

Ethics is about "the decision making and actions of free human beings" (Laudon, 1995:34). In the simplest terms, ethics is about what is considered to be right and what is considered to be wrong. Although the field of ethics is subjective, society has, in general, been able to agree on what is and is not acceptable in our culture. Most ethical systems are based on values common to the majority of society, as evidenced by public laws enacted by the people to punish those behaving in a manner contrary to these mores. Common values underlying our culture are also exhibited in recurring themes found in professional ethical codes. Today, however, rapid advances in information technology are providing a new challenge to traditional considerations of what is right and what is wrong. This challenge derives, in part, from the increased access to information and greater range of professional and recreational choices offered by current information technology. The ethical principles that apply for many of these choices have not yet been agreed on. Today's organizations, in both private industry and government service, are facing unprecedented ethical issues in the workplace emerging from the use of advanced information technology, specifically, ethical issues involving networked information systems (Barbour, 1993:xvi).

Key ethical issues regarding computers and information systems are not new—they are simply a "new species" of traditional moral issues (Johnson, 94:10). Many of the issues discussed in both the private and public sectors have been addressed in the past. Some of these situations have clear ethical implications while others are more subtle. In 1986, prior to the widespread implementation of networking, Richard O. Mason summarized the four primary ethical areas for the information age as privacy, accuracy, property, and accessibility (PAPA) (Mason, 1986:5). By 1994, during the rapid infusion of data communication networks, Johnson asserted these same traditional concepts were indeed the key issues surrounding computer ethics but with an increased scope: "The issues in computer ethics can be categorized using traditional concepts: privacy, property, crime and abuse, power and responsibility, accountability and liability, and professional practice" (Johnson, 1994:11). However, she cautions that "we cannot simply and mechanically apply traditional legal and moral principles to cases involving computers" (Johnson, 1994:5). She contends we must first reconcile the unique characteristics of information technology with our understanding of its capabilities and differences from traditional technologies (Johnson, 1994:5). By doing so, "we can see situations involving computers in relation to our traditional moral norms and values" and establish meaningful policies and rules (Johnson, 1994:5). To ensure an environment of ethical network usage, the USAF must understand the advanced capabilities of networks and identify which unique characteristics apply to users of USAF networks. An understanding of the unique capabilities applicable to the workplace can enable USAF planners to begin to look at the ethical issues surrounding advanced information technologies.

Why Should the USAF Be Concerned With This Ethical Quandary?

The primary ethical issues pertaining to information technology in the workplace today, privacy, property, accuracy, accessibility, crime and abuse, power, responsibility, and accountability are pertinent to information networks due to the unique characteristics of networking technology. These characteristics include scope or power, anonymity, reproducibility, and autonomy (Johnson, 1994 and 1997; Loch and Conger, 1996; Abshire, 1982; Rubin, 1996). These characteristics interact with each other to provide the basis for the "new species" of traditional ethical issues regarding current information technology. Together these characteristics constitute the unique aspects of a networked work environment which, although similar in some respects, is much different from the work environments of the past. Just as Geison observed in his 1996 study that "electronic documents are not merely digital pieces of paper," electronic networks are not simply a digital work environment—the entire nature of the environment is fundamentally different (Geison, 1996:6).

Unique aspects of current information technology are due in large part to advances in communications technology. The proliferation of telephones, radios, television, copy machines, and facsimile machines through the years has exponentially increased the span of communication around the globe. A primary difference between traditional information technologies and networking capabilities of today is the tremendous scope and power an action—a communication or transfer of information—performed on a network can have compared to an action in ordinary, physical space (Johnson, 1997:62). Johnson refers to scope as a combination of broad reach, immediacy, and interactivity of users (Johnson, 1997:61). Networks have provided the ability to communicate directly with other users, linking individuals across national and international boundaries as easily as if they were across the street (Langford, 1996:91). Although a great convenience, this tool is capable of performing powerful actions. If not used appropriately, this powerful tool can lead to financial loss, tarnished reputations, and possible legal action for both individuals and organizations (Kallman, 1992:69).

In conjunction with increased scope, current information networks can promote a sense of anonymity. Network usage and capabilities such as electronic mail and bulletin board/newsgroups have eliminated much of the face-to-face interaction that used to take place in the workplace. This elimination of human contact can promote a loss of awareness or a moral distancing on the part of the user and the consequences of his or her action. This distancing may tempt users to try to access unauthorized information, harass another user, or otherwise misuse network resources (Rubin, 1996:126). In addition, a loss of awareness can prompt users to be more "insensitive" by not considering the consequences of the actions they are taking (Abshire, 1982:10).

Reproducibility in the physical world requires a different type of effort by an individual than reproducibility in an electronic world. Using a copy machine and hand copying files are observable actions with tangible, physical aspects to them. Although copying a file on a network also uses the physical items of a computer, keyboard, monitor, and wires, it is a more secluded activity which is observable only if one is watched closely. In addition, the reproduced copy not only is identical to the original file, but the original file may not exhibit any signs of being copied. Reproducibility pertains to the characteristics of autonomy and independence because users can feel more secluded or autonomous when operating in a networked environment. The independence granted to users in a networked environment can promote the feelings that the user is isolated from others. This isolation may lead the user to feel he or she is isolated from the consequences of actions taken on the network, which in turn could lead to the performance of unethical acts.

Importance of Issue

"The Air Force exists to fight and win wars… We're entrusted with the security of our nation" (Fogelman, USAF Core Values, 1997). However, no matter how lethal the tools the USAF is entrusted with, no matter how risky the operations we engage in, the USAF operates under a microscope. This scrutiny is due in part to budget crises, personnel cutbacks, and public scandals—what General Fogelman calls our "big ticket scandals" (Fogelman, USAF Core Values, 1997). Whether we have lost dedicated personnel in a senseless crash, mistakenly shot down our own aircraft, or a member has publicized personal problems in the media—the situation ultimately tarnishes the overall image of the entire service. Because the USAF is operating under such scrutiny, the service cannot afford to present even the perception of abuse or unethical behavior when it comes to the use of government-sponsored resources. "The Air Force recognizes its critical role in promoting the general welfare and we fully understand that Congress and the American people expect us to maximize the return on each taxpayer dollar" (Air Force Issues Book, 1995).

The USAF, like other agencies of the federal government, has invested a substantial amount of resources in the installation and maintenance of networked information systems available to a majority of USAF personnel. To ensure these systems are not improperly used or abused, ethical issues regarding network usage must be addressed at all levels. The management level must include an effort to balance these issues ensuring network policies allow for some judgment by network users. At the user level, one of the most important issues to address is that users must realize that business in a networked environment are not business as usual. Users at all levels must make certain networks are used in a manner appropriate to the core values of the USAF. To act in an appropriate manner, users must be aware of how networks are different from traditional means of doing business.

Today's network technology allows easy access to many different information choices that were previously unavailable in the workplace. In the USAF several individuals have been investigated, charged, and convicted for inappropriate use of government computer networks. Charges include downloading inappropriate information from the Internet, compromising passwords for USAF systems, and using an organization's computer system to recruit top people to moonlight for a private company owned by a high-ranking civilian. A surprising fact is that those convicted are not just young airmen new to the workplace who do not know better. Those convicted include a base commander (colonel), a captain with 23 years of service, and a master sergeant with 19 years of service. Senior officers and airmen should be setting the example for the young troops, not misusing government resources. Recognizing the unique characteristics of network resources can help all users realize the potential ramifications of improperly using government networks.

The previous examples indicate that a key focal point in computer abuse and misuse is the individual user. Concepts of Total Quality Management (TQM) and advances in information technology have enabled organizations to empower lower-level employees to make more of their own decisions. By doing so, users have also been empowered to assume greater responsibilities with reduced supervision, granting users increased independence in the performance of their duties. Empowerment and independent access to a wider range of choices become critical factors to the USAF as its base of internal users expands due to the increased outsourcing to the private sector. This expansion of internal users increases the threat of abuse and misuse by those with authorized access to USAF systems. The ethical use of computers and information networks by USAF authorized internal users must be addressed to ensure users operate, support, and maintain a networked environment consistent with USAF values.

Workers are now provided more autonomous access to information systems than in traditional work environments. This access, along with the empowerment of low-level users and independent operation of a networked system, can lay the groundwork for conflict within the workplace. To operate successfully in a networked environment, managers must place a great deal of trust in their subordinates. One of the most important issues for the USAF is to ensure users do not misuse the systems at their disposal. To reduce the risk of USAF network abuse, users must be made aware of the unique characteristics of the current information technology, the possible impact of the implementation of these systems, and the potential ramifications if these systems are misused.

Problem Statement

The USAF must address many issues in the area of expanding information technology usage. This thesis attempts to first identify characteristics and ethical issues surrounding network usage, and then evaluate current Department of Defense (DoD) regulations and Air Force Instructions (AFI) regarding network usage to determine if they address these issues. In addition, the research will also attempt to determine if USAF members consider networked systems to be significantly different than traditional means of doing business or whether they are simply novel tools to perform their duties a different way. The scope of this thesis is limited to the ethical aspects of networks because it is currently one of the primary areas that must be dealt with by virtually all USAF employees. Managers and supervisors must be aware of the threats to their individual areas due to networking, while individual users must be familiar with the unique aspects of networking. Users must be aware of what activities constitute misuse of information networks and the consequences of using the systems inappropriately. The USAF and its members need to be familiar with the emerging field of computer ethics because "our standards *must* be higher than those of society at large. The American public expects it of us and properly so" (Fogelman, USAF Core Values, 1997).

This research addresses the significant ethical issues surrounding the use of information networks. The thesis reports the results of an exploratory investigation regarding perceptions of the ethical implications of using networks. The analysis of the data provides a preliminary understanding of how USAF users perceive information networks in terms of network capabilities and how the USAF is addressing corresponding ethical issues. Specific investigative questions addressed in this study include:

1. To what extent do the unique capabilities possessed by information networks contribute to a fundamental difference between a networked work environment and a traditional paper-based environment?

2. What are some of the ethical issues involving the use of information networks, how are these issues different from a traditional work environment, and how has the USAF addressed these issues?

3. Do USAF network users concur in their perceptions regarding activities in a networked environment?

The results of this study will help the USAF identify information practices that have the potential to raise concern in the public eye and assist the USAF in understanding how to address concerns about inappropriate network usage.

Summary

Both academic studies and popular literature include many works regarding the ethical issues involving the vast expansion and rapid mainstreaming of information technology (Abshire, 1982; Forester and Morrison, 1995; Johnson, 1994 and 1997; Kizza, 1996; Mason, 1986; Neumann, 1995; Nissenbaum, 1994). A significant amount of literature exists focusing on the ethical responsibilities of computer designers and programmers (Baase, 1997; Kling, 1996; Weckert, 1997). Recent articles, however, indicate a trend toward more interest in the area of end-user responsibility (DeJoie, 1991; Forester and Morrison, 1995; Johnson, 1997; Neumann1995). Chapter II addresses the background question of: what is computer ethics? This chapter explores the basic issues underlying the subject: what are the ethical issues regarding information technology and networking, what makes these issues different from ethical issues prior to network capabilities, and how can they be addressed and answered? This chapter addresses the ethical principles surrounding individual computer and network usage.

This research focuses on an exploratory study of various organizations/users on one USAF base to identify and compare individual user perceptions of the unique ethical issues in a networked environment. To obtain data on user perceptions of a networked environment, a sample of users on Wright-Patterson Air Force Base (WPAFB) was surveyed. This survey, described in Chapter III, attempts to provide a preliminary idea of user understanding regarding network usage currently present in the workplace. Chapter III addresses the methodology chosen and its suitability for this topic.

Chapter IV then details the responses to a survey administered to members assigned to WPAFB to gain their perception of the ethical issues surrounding network usage. This three-pronged approach, a discussion of the issues and features regarding network usage, the policies enacted by DoD and the USAF, and the survey responses, provides a preliminary assessment of how the USAF is addressing the issues identified by the professional information technology community. This assessment can help the USAF determine whether the service is at risk for increased unethical behavior by USAF members when using government-sponsored networks.

Chapter V presents the results of the study and answers the question: What does this data regarding user perceptions of a networked environment convey about the workplace in the USAF today, and does this data correspond with issues discussed in the literature review? In addition, this chapter provides observations and conclusions for USAF managers to assist them in guiding and managing individuals in their usage of government-provided information technology. Chapter V also provides the limitations of the current study and recommendations for future research efforts.

II. Literature Review

Introduction

Communication via computers is not a revolutionary concept. The recent exponential increase of this activity, however, has reached the point that for many people, electronically distributed communication supplants the postal service, telephones, and even fax machines (Boudourides, 1995). The dramatic growth of distributed communication available through computer networking is illustrated by statistics developed by the Internet Society, a "non-governmental international organization for global cooperation and coordination for the Internet and its networking technologies and applications" (Rosenberg, 1997:87). This organization estimated a worldwide figure of 130,000 Internet hosts in 1989—a figure which dramatically increased to over 16.1 million as of January 1997 (Rosenberg, 1997:84).

The USAF has recognized the importance of information technology and networking to its mission. Former USAF Chief of Staff General Ronald Fogelman considered the "technology information explosion in our society" as a signal that the USAF was crossing a new frontier—calling information operations "the fifth dimension of warfare" (Fogelman, 1995). Air Force Policy Directive 33-2 dated 1 December 1996 states "information demands to support Air Force operations have intensified at an exponential rate—to satisfy this demand, the Air Force needs a transparent infosphere that must provide accurate, timely, and secure information in any required form, at any time and place" (AFPD 33-2). This infosphere has been in large part enabled by the development of networking technologies. The increased interconnectivity of computer networks during the last decade has enabled the USAF to build this infosphere to accomplish its mission.

This chapter identifies the unique features of computer networks and discusses the ethical issues regarding network usage as outlined by the academic community. This discussion includes how these issues differ from those found in traditional work environments. The chapter concludes with a review of the policies implemented by the USAF and WPAFB regarding the use of USAF computer networks and whether these policies sufficiently address the issues discussed.

Networking Implications for the Military

Networking is a combination of two traditional technologies, computers and telephones. During the latter part of the twentieth century telephones have become instrumental to virtually every part of society. Computers—like telephones, automobiles, and radios—have changed the way we work, play, and organize our lives (Baase, 1997:2). Computer technology has the power to make routine tasks quick, easy, and accurate. Information technology allows the easier management of finances, the quicker consideration of options, and more rapid preparation of financial statements, forms, and reports (Rosenberg, 1997:56). This technology also enables the organization and access of information more quickly and efficiently. Interconnected computers use telephone connections to allow people to transfer information over networks (Resnik, 1996:16). Although local computer networks have existed for many years, today a global network exists connecting people all over the world. There is nothing new about networking (Resnik, 1996:16). There is nothing you can do on a network you cannot do with a telephone, printer, fax, camera or voice; however, unique differences between networking and other, more traditional forms of communications technology exist (Resnik, 1996:16).

A key issue for the USAF in regard to computers and a networked infosphere is the role of the end-user. Computers and especially networking have enabled end-users to have a significant amount of power at their fingertips. Networking technology has created opportunities for unethical actions and illegal activities that were not even considered prior to its existence (Baase, 1997; Forester and Morrison, 1995; Johnson, 1994; Kling, 1996). Computer technology has opened up radically new opportunities, such as high-speed communication, global searching of enormous databases, junk e-mail, and undetectable surveillance of information exchanges (Neumann, 1995:275). Users can communicate with others at their convenience, sending immense quantities of information quickly without visible, physical evidence they have done so (Resnik, 1996:16). Users can also gain access to massive amounts of information from all over the world that would not be physically available to them in a traditional work environment. This capability has enabled a certain amount of productivity; however, there is a concern that as end users have been enabled to be more productive using networks, they are also now able to perform certain kinds of abuse and cause certain types of damage.

Providing networked system access to employees requires organizations to place a great deal of trust in their workforce. Unconstrained communication and rapid interactions entail risks including intentional and unintentional abuse as well as "emotional, simplistic, or knee-jerk responses to complex issues, sometimes with irreversible consequences" (Neumann, 1995:279). Seemingly harmless abuse such as software and information duplication can be propagated more easily (Neumann, 1995:279). Losses due to computerized fraud and theft are many times larger per incident than those from non-computerized fraud and theft (Fitzgerald and Dennis, 1996:426). FBI data show that for the past five years the average loss for bank robbery was around $3,000, while the average loss from computer fraud was approximately $300,000 (Fitzgerald and Dennis, 1996:426).

Unauthorized access to information is a serious risk. Unauthorized access is a threat not only from external users "hacking" into a system but from authorized internal users. Although a popular perception is that hackers cause the greatest damage to systems, less than 25 percent of all unauthorized access incidents involve outsiders; 75 percent are insiders—authorized system users (Fitzgerald and Dennis, 1996:428). Department of Defense officials are concerned about insiders because the insiders know the organization's weaknesses and occasionally try to take advantage of what they feel may be an easy target or victim (Hamblen, 1996:4). During this era of personnel reductions "disgruntled workers may try to walk away with everything from memory chips and software to entire computers" (Hamblen, 1996:4).

Current information technology, networking in particular, has enabled the collection, maintenance, and more importantly, distribution of more information than would be logistically possible without electronic storage and information retrieval. This development is especially important when it comes to information regarding national security. Convicted spy Aldrich Ames testified that network access was "a significant event in his espionage career because it allowed for a substantial increase in the amount of data he could carry out of the building with reduced chances of detection" (Hamblen, 1996:5). To add some perspective to this situation: Ames could fit more information on a single floppy disk than the ten pounds of classified material John Walker wrapped in a black plastic trash bag and placed under a bush (Hamblen, 1996:5).

Organizations must be vigilant of their online systems, not only to maintain their information but to ensure it is not compromised or altered. In 1995 the Naval Security Group (NSG) calculated that gaining access to 11 percent of the United States Navy's networks can compromise 97 percent of unclassified navy systems (Hamblen, 1996:6). In the same year the USAF Computer Incident Response Team (AFCIRT) recorded 2,500 intrusions of USAF systems (Hamblen, 1996:6).

Unauthorized access can also happen unintentionally or inadvertently. The USAF must ensure those who manage the distribution of information through official USAF sponsored network sites are aware of the ethical issues that may arise in the course of their duties. The intangible nature of information makes it almost impossible to know who gained access to information that was distributed over a network or located on a World Wide Web page. In 1997, Headquarters, USAF released the results of an audit that revealed problems in the control of official network bulletin boards and home pages. A key finding was that "several home pages displayed or provided links to inappropriate information" such as "commercial sleaze" and "gossip web sites" (HQ

USAF, 1997). In addition, some home pages displayed unauthorized information such as the types of weapons maintained in that installation's armory. Others provided information that violated the Privacy Act or the Freedom of Information Act.

Releasing information without proper authority is a violation of USAF directives and in some cases, Public Law. Prior to information networks and the existence of home pages, individuals would require an authorized signature or the approval of the Public Affairs office before publishing information or providing information to the general public. The convenience of networking does not preclude standard authorization policies. According to the message released by Headquarters, USAF with instructions for "widest dissemination:"

> Releasing information without proper authorization violates regulations and is both embarrassing and detrimental to the USAF.... Links to inappropriate information bring discredit to the USAF and may be construed as an official USAF endorsement of these activities.... We need close personal attention of the accountable supervisors to prevent this from happening. Personnel must be reminded that they leave "electronic footprints" when they use a network. (HQ USAF, 1997)

This posture taken by Headquarters USAF is pertinent not only for officially-sponsored information available on an information network, but also for the actions of individual users when using government-sponsored information systems.

Military Members and Network Usage

"*Web Surfing Officer Nets Nine Months Confinement*" (Air Force News Service, 11 Feb 97)

"*Officer Dismissed for Computer Porn*" (Air Force News Service, 9 May 97)

"*Don't Chat, Don't Tell? Navy Case Tests Privacy Limits*" (Simons, Wall Street Journal, 14 January 98)

"*Master Sergeant is Sent to Jail in E-mail Case*" (Compart, Air Force Times, 10 Jun 96)

"*Computer Expert Gets Hooked on Child Pornography via Internet...Courts-martial Results in Airman Losing More Than Just His Career*" (Lozo, Command Post, 8 Nov 96)

"*Computer Crime...Soldier Faces Courts-martial in Espionage Case*" (Brewin, Federal Computer Week, 26 Aug 96)

The above articles are cited from commercial, federal, and military publications. Each involves the use (and misuse) of computer networks by military members. In these cases, usage of the networks took place during both on- and off-duty hours. However, the specifics of each case differ in that although most of the cases involve the direct misuse of a government computer network, at least one of the members was using his personal user account on his personal computer system in the "privacy of his on-base dorm room" (Lozo, 1996). In the Navy case, an authorized transmission over a government computer network led authorities to track a user identification account through a commercial on-line system. Navy investigators allege the senior petty officer with 17-years service had entered *gay* under the heading of *marital status* on the profile for the commercial system and had therefore violated the *don't ask, don't tell* policy instituted by the Commander-in-Chief for all military members (Simons, 1998). These cases indicate the potential for unethical network actions within the USAF due to the unique features of networking.

Unique Features of Network Technology

When new technologies are introduced, the overall ramifications of their adoption are typically unpredictable (Ladd, 1997:9). For example, widespread use of the automobile is credited with the rise of the suburbs while jet airplanes have been credited with playing a large part in the globalization of the world's economy (Ladd, 1997:9). In the tradition of the printing press, railroads, automobiles, and telephones, developments in information technology over the last few decades have dramatically affected society, particularly the workplace. As opposed to these more traditional technologies, however, computer technology, particularly networking, embodies unique characteristics. These characteristics distinguish networking from traditional communication methods such as face-to-face, printed paper, telephone, fax, and mass media (Johnson, 1997:61). These unique features include a broader scope than other technologies, the perceived anonymity of network usage, the unprecedented autonomy now present in the workplace, the significant barriers to accountability in a networked environment, and the ease of reproducibility on a network (Barbour, 1993; Johnson, 1997; Jones, 1991; Nissenbaum, 1994; Rubin, 1996). Although each of these characteristics is not unique by itself, working in conjunction with each other the combination seems to be the overall factor in the uniqueness of networking. Each of these features interacts in a networking environment creating a novel, powerful kind of information technology that presents tremendous temptations (Resnik, 1996:19).

The Special Scope of Networked Systems. A primary difference between traditional information technologies and networking capabilities of today is "the tremendous scope, or power, an action—a communication or transfer of information—performed on a network can have compared to an action in ordinary, physical space" (Johnson, 1997:62). Johnson refers to scope as a combination of the vast number of people reached, the immediacy with which an action can be taken, and the ability of many individuals to interact with each other (Johnson, 1997:61). Users can access a much broader information base with little effort as compared to the past—they do not have to physically go to the library, bookstore, or local newsstand to get information they want. In addition, users have incredible computing power literally at their fingertips—the capability of reaching thousands of people with one message compared to placing hundreds of phone calls or mailing hundreds of letters.

Communication in a networked environment is significantly different than that of the non-networked world. Producing a traditional document involves several steps and stages. At each stage the author may modify the text or even "scrap the whole idea" (Langford, 1996:97). This extended process doesn't fit the generation of electronic documents, which are quick and easy to produce: "Many people create and send e-mail spontaneously, often without pausing to consider use of tone, language, or even if the message is really appropriate or necessary" (Langford, 1996:97). With a personal computer, modem, and specific software actions can cross international boundaries as easily as city, state, or national boundaries (Bordia, 1997:99).

In the physical, non-networked world it may be on the order of ten times as much work to mail out ten items as it is to mail out a single item. On a network it may be just as easy to send an item to thousands of places as it is to send it to one location. Current information technology enables users to get a message to another country as easily as to another neighborhood. Without having to bother with stamps, envelopes, and the delay of the postal service, millions of people have interacted via e-mail (Bordia, 1997:99). Although a great convenience, networking is a powerful tool capable of performing powerful actions. If used inappropriately, this tool can inflict significant damage upon an organization through the unauthorized access or theft of information, improper representation of an organization, or simply misapplied man-hours.

At present computer networks are generally seen to be tremendously powerful tools (Huff, 1996; Johnson, 1997; Langford, 1996; Resnik, 1996). Huff defines power in a physical sense power as "the potential to do work" and in a social sense as "the ability to influence others" (Huff, 1996:8). Computer networks fall into both the physical and social definitions of power. The power afforded by networking enables an action to have a much broader scope, to be accomplished with tremendous speed, and to reach a potentially limitless number of other users. The inherent power of networking technology is indicated by Langford:

> All users connected to a network have the ability to publish whatever they wish to every other network connected individual. Established network users believe this ability is so powerful it must always be limited and used with considerable care and foresight. Of course, there is no technical way to prevent global distribution and this restriction may be ignored without legal penalty. (Langford, 1996:98)

If the care and foresight mentioned by Langford is not practiced when operating in a networked environment, it may be difficult to see all the potential consequences of an action when it is actually performed. This difficulty may be because the initiator of the action can be so far removed, or distanced, from the end result. Huff refers to this situation as unintentional power. Unintentional power is associated with our actions whenever those actions have unintentional consequences (Huff, 1996:8). In situations where the end result is so far distanced from the user it may be difficult to assign responsibility or accountability to the originator of an action (Huff, 1996:7).

Anonymity in Networked Systems. In conjunction with increased scope, current information networks can promote a sense of anonymity. Network usage and capabilities such as electronic mail, bulletin boards, and newsgroups have eliminated much of the face-to-face interaction that used to take place in the workplace. Networked environments instead depend on computer-mediated communication or CMC. As opposed to face-to-face interaction, CMC is primarily textual:

> there are no nonverbal cues to embellish the meaning or social context cues regarding gender, age, or status. Not only can the absence of cues hamper communication efficiency, but it seems to create a semblance of anonymity and lack of awareness of the social context. These conditions, in turn, have been held responsible for a perceived higher incidence of rude, offensive, and uninhibited behavior. (Bordia, 1997:100)

Because people cannot see or hear others laugh, wince, or indicate any other psychoemotional reactions to their actions, they can become more socially insensible (Boudourides, 1995).

The very nature of networking allows for a certain level of personal anonymity. “This feature leads to many of the difficult ethical and legal questions society is now beginning to face" (Resnik, 1996:17). Anonymity in networks may encourage users to utilize a pseudonym, take on a different persona, or take on someone else's identity (Johnson, 1997:62). Off-line anonymity requires physical effort to remain anonymous while anonymity is a natural state in an online world (Johnson, 1997:62). In addition, integrity problems arise because anonymity disconnects a person from his words and actions (Johnson, 1997: 62). In an online environment it is hard to establish the integrity of information. Users can never be 100 percent sure if the words they receive are the sender's words or someone else's. If users don't know the sources of their information they can't develop a history of experience with the source. Without that experience people cannot make fully informed decisions, and they do not know what information they can rely on (Johnson, 1997:64). The off-line world also deals with problems of integrity but comparable disconnects require different physical behaviors (Johnson, 1997:62).

The anonymity available to users on a network may have significant ethical implications. In highly automated offices, workers don't have the social interactions they once had when they had to manually coordinate their work. In some organizations staff meetings have become a thing of the past because notes and announcements are forwarded over the network. When workers communicate without face to face contact, trusting relationships don't develop (Johnson, 1997:64). A lack of social interaction can lead to employee isolation. If employees feel they are alone all the time they could be tempted to do something they normally wouldn't do.

Isolation, which may develop by working in a technology-intensive environment, can lead to a condition of deindividuation (Loch and Conger, 1996:76;

Bordia, 1997:100; Lea and Spears, 1991:284). Deindividuation is the feeling of being estranged or separated from human contact—"users lose awareness of others which may lead to behavior violating established norms of appropriateness" (Loch and Conger, 1996:76). An individual in this state may have heightened feelings of anonymity that may lead to fewer inhibitions concerning socially unacceptable acts (Loch and Conger, 1996:76). This condition, even in a mild form, contributes to the characteristic of insensitivity, because "computer induced deindividuation appears to reduce the computer user's ability to identify other stakeholders of their actions" (Abshire, 1982:10; Loch and Conger, 1996:76). This situation can prompt users to be more insensitive by not considering the consequences of the actions they are taking (Abshire, 1982:10). Users more frequently engage in antisocial and unethical behavior if others affected by the action cannot be identified (Loch and Conger, 1996:76). Of the following, the easier, least conspicuous action is to send a virus over a network instead of walking into an office and smashing the computer with a sledgehammer (Resnik, 1996; 17).

Elimination of human contact can promote a moral or psychological distancing of the user from the consequences of an action he or she has taken (Resnik, 1996:17; Rubin, 1996:126). This distancing occurs when technology allows people to interact without the benefits and burdens of face-to-face contact (Resnik, 1996:17). Anonymity and lack of human feedback (gestures, nods, tone of voice) erase established conventions and norms for interaction (Boudourides, 1995). Networking brings about distancing in human communication (Resnik, 1996:17). Distancing "makes it harder for people to feel empathy and easier for them to inflict suffering, more likely to feel apart from the community, less likely to identify with peers, and more likely to feel isolated" (Resnik, 1996:17). This distancing from the end result of an action can tempt users to try to access unauthorized information, harass other users, or otherwise misuse a network (Rubin, 1996:126).

Rubin illustrates the concept of moral distancing using an analogy borrowed from the tradition of the USAF:

> This sense of moral distancing was sensitively characterized in a poem by American poet James Dickey.... In his poem entitled "The Firebombing," the central voice is an American World War II bomber pilot who is in the act of dropping firebombs on the Japanese countryside during what is called an "anti-morale" raid.... What is striking about this poem is that the pilot, far above the exploding and burning ground, in a cockpit darkening with twilight, spends his time admiring the beauty of the evening, and from his safe altitude, the beauty of the incendiaries that detonate below. The pilot speaks:
>
> > ...[W]hen those on earth
> > Die, there is not even sound;
> > One is cool and enthralled in the cockpit,
> > Turned blue by the power of beauty,
> > In a pale treasure-hole of soft light
> > Deep in aesthetic contemplation,
> > Seeing the ponds catch fire...
>
> The pilot is unable to see the carnage that is created on the ground, because the characteristics of the technology and the physical environment in which he is operating divert him, literally blind to the fiery reality below.
> The moral distance that is created is caused by many factors: first, anonymity, for no one below can see the pilot, therefore he is free from faces that would no doubt haunt and accuse him if he could see them; second, the physical distance from the ground itself obliterates the awful details of what is happening below.... (Rubin, 1996:126-127)

Rubin goes on to ask, "if such great destruction can escape our moral attention, could similar characteristics in more mundane settings even more easily distract our moral compass?" (Rubin, 1996:127) This powerful analogy provides a profound example of how anonymity may distance people from the ethical ramifications of their behavior.

Autonomy in a Networked Environment. The advent of networking has enabled organizations to decentralize computing power. This is a relatively new phenomenon for many organizations. Prior to the widespread use of stand-alone and networked computers, many organizations either accomplished work manually or by enormous mainframes that were centrally controlled. This central control has been dispersed throughout organizations due to the unprecedented distribution of computing power and new management philosophies of empowerment and quality management. In an era of downsizing (or rightsizing), organizations are attempting to do away with the rigid, hierarchical structure in the tradition of Frederick Taylor. Organizations are attempting to flatten established frameworks to reduce middle management. Ideally this effort is supposed to empower employees to make decisions without having to wade through a complicated bureaucracy. "For the many working people whose autonomy is routinely challenged by the constraints of large organizations or the vagaries of the market, the spread of sophisticated computers holds the promise of gaining personal control" (Clement, 1994:53).

In keeping with the idea of empowerment and the promise of more personal control, networks have opened up wide, uncontrolled avenues to the outside world from deep within organizations. Workstations have put control in the hands of the individual user, not the organization. Workers not only have access to a greater amount of information from within the organization, but they also have access to see what is going on in the world outside their organization. Unless a manager's span of control is extremely small (one or two people) it is nearly impossible for him or her to know what each person is doing on his or her computer at every minute. Since there is no way to effectively control every transmission and action the workforce takes without bringing business to a virtual halt, managers must be as knowledgeable about the network and its systems as their subordinates. This is a radical change for the traditional manager who previously only had to supervise production and not worry about the workings of how a job was accomplished as long as it happened. This change counters traditional concepts of work and management and therefore may create a serious dilemma for managers and especially the executives responsible for the organization.

Managers run the risk of employees not completing their assigned tasks because they become engrossed in surfing the Web or worse, because they are compromising organizational information to a competitor or adversary. An issue arising from this conflict between managerial trust and user independence regards the extent to which USAF employees are allowed to use networks for other than official business. Is there or should there be a middle ground? A middle ground would allow employees to use the network to facilitate personal business at a reasonable level—especially if it would be the most efficient use of the user's duty time. Headquarters USAF has defined this middle ground as when network use "serves a legitimate public interest, such as keeping members at their workstations, improving morale, enhancing professional skills, or furthering education" (HQ USAF, 1997).

Decentralization of computing power within a workforce is a relatively new phenomenon for many organizations. The widespread application of networking has taken the workplace by storm. Proponents of information technology advocate for both the public and private sectors to use as much technology as they can to enable organizations to be competitive in the 21st century. They appeal to a business' bottom line of profit by promising that computers can allow the company to do more work faster and cheaper than traditional business methods. Competition in the marketplace is intense and innovative with new offerings appearing on a monthly, even weekly basis. Unfortunately the decentralization of computing power and new information networking have outpaced most organizations' abilities to effectively meet the challenge of issues such as ethical behavior in the use of the network.

Bureaucracy and red tape have become synonyms for government agencies in our society. In the military, members are used to having to obtain approval from at least one level above themselves to perform any action which is not part of the standing operating procedure. The promise of networked computers to empower individual users and put control in the hands of individual users is a radical idea for military members at every level. Leaders of higher rank, such as commanders, will expect that actions that could possibly compromise a unit or an entire organization will be passed through them for approval. This approval most likely will be expected in the form of an official memorandum or letter—a tangible piece of paper that must be signed to signify approval. These higher-ranking individuals may not even realize the capability to do otherwise exists without a great deal of work. Those members of lower rank who are dealing with the new networked environment every day may take for granted actions that are easy and convenient via networks. These members may not realize specific approval may be needed for certain actions.

The autonomy or independence offered by networks can be potentially dangerous for the military. If, as Clement states, empowerment seeks to "give staffers a potentially unbounded scope to participative rights on all matters that directly affect them," then the entire purpose of the military is jeopardized (Clement, 1994:61). As Geison noted in his study on hypertext:

> If the USAF does transform its publications into hypertext, users would be likely to have a direct opportunity to immediately challenge the authority of a text. An e-mail link, for example, to the office of primary responsibility could easily be included within a hypertext document. ...When the user can ask "Why?" with the click of the keyboard, one can expect that many users will take advantage of the opportunity. This process may well subtly erode the authority of the text. ...Directives will seem to come from an easily accessible individual who one can challenge and disagree with in virtual real time. (Geison, 1996:58)

The use of hypertext is a primary means of communication over a network. Official publications are the rules USAF members live by. The idea of every member being able to challenge each piece of documentation is an invitation to the degradation of good order and discipline. In this type of environment, members may feel distanced from the potential ramifications of questioning authority or disobeying orders. The military exists to execute orders issued by elected officials to support national policy objectives. If every airman, soldier, and sailor is to be empowered to promote his or her own policies or opinions on a network, the military would become completely ineffective. The military must exert some form of control over networking to ensure service members do not perform inappropriate actions nor are allowed to dispute authority.

Barriers to Accountability in a Networked Environment. Society has become more dependent on computers and computer networks. As this dependence increases we also become more vulnerable to computer malfunctions and to misuse of computers and computer networks by human beings (Forester and Morrison, 1995:1). Computer misuse can lead to many negative consequences ranging from physical harm to wasted time. When any type of computer malfunction or misuse occurs, we want to know who is accountable—we want to know what went wrong, why it went wrong, and who will pay for the damages (Johnson, 1994:126).

According to Johnson, to say that someone is accountable for an action is "simply to say that he or she is the appropriate person to respond when something undesirable happens" (Johnson, 1994:127). The inherent complexity and potential anonymity provided by computer networks can make it difficult to determine who performed an action on a network. The types of behavior that have become problematic on computer networks include defamation, distribution of pornography, harassment, and posting of information that assists crime (Johnson, 1994:141). These types of behavior are illegal off-line, yet they pose a special problem on a network since it is difficult to determine who performed the action (Johnson, 1994:141). In these situations the criteria normally used in assigning responsibility or accountability are unable to be used.

Helen Nissenbaum claims that computerization is undermining accountability (Nissenbaum, 1994:73). She claims that those who are answerable for harms or risks are the most driven to prevent them (Nissenbaum, 1994:74). However, in an electronic environment it is often difficult to discover who actually performed the action leading to a lack of accountability. By computerizing all tasks and connecting everyone to an information network, there is little motivation for those who work with those networks to ensure the accuracy and integrity of the system. Nissenbaum identifies four reasons why computer systems are diminishing accountability. She refers to these as the "four barriers to accountability" (Nissenbaum, 1994:75).

The first barrier is the problem of *many hands,* where responsibility is diluted because so many in the organization have access to the system, a problem of collective responsibility (Nissenbaum, 1994:75). The second is the issue of bugs. Because computers have become such an integral part of our lives, there is a degree of error that is viewed as inevitable. Nissenbaum claims an attitude has developed that since software errors are a "natural hazard to any system" and are for the most part unintentional, it is "unreasonable" to hold developers accountable for any imperfections (Nissenbaum, 1994:75). The third barrier is one which is common today—using the computer as a scapegoat (Nissenbaum, 1994:75). This is common in an electronic environment, since some individual's job is dependent on a computer database or network. This barrier can range from the bank not being able to provide an account balance because the computers are down to the terrifying thought of the air traffic control system at a major airport malfunctioning resulting in the lack of coordination for airplane departures and landings. The final barrier is that of ownership without liability or, having your cake and eating it too (Nissenbaum, 1994:75). An example of this barrier is that most software producers want ownership rights to software they develop. However, these same producers do not want to accept responsibility or liability for the software if it malfunctions (Nissenbaum, 1994:75).

Reproducibility in a Networked Environment. Reproducibility in the physical world requires a different type of effort by an individual than reproducibility in an electronic world. Using a copy machine or hand copying files are observable actions with tangible, physical aspects to them. Although copying a file on a network also uses the physical items of a computer, keyboard, monitor and wires, it is a more secluded activity that is observable only if one is being watched closely. In addition, the reproduced copy not only is identical to the original file, the original file won't exhibit any signs of being copied. Another incentive to reproduce material on a network is that computers allow the transfer of immense quantities of information for relatively low cost. For the user using a system at work there is often no cost since the users don't get the bill for the system, the organization does.

Reproducibility can lead to justification of stealing another's information or pirating software. In the physical world information can be reproduced but not as easily and as transparently as in the electronic world (Johnson, 1997:62). The person who created or owns the information may have no idea it was copied. Even if the victim did realize the information had been taken, finding the thief would be difficult; fingerprints in cyberspace are much more difficult to lift. Reproducibility also creates a possibility of permanence or the endurance of information on a network which can be taken and used by someone else (Johnson, 1997:63). This feature confronts our traditional ideas of property and personal privacy--the idea of control. Once an action is in cyberspace effort is required to remove it, in the off-line world, effort is required to record an action (Johnson, 1997:63).

A Final Word on Unique Characteristics. The scope of decentralized network-computing power, the increasing anonymity and isolation of the workforce, and the ease of non-accountable reproducibility are only some of the unique characteristics of networked environment in which organizations operate today. While other forms of technology share some of these unique features (phone, radio, television, etc.), networking technology alone provides the striking combination of these features

(Johnson, 1997; Resnik, 1996). These features could tempt people to justify improper actions while trying to add some "excitement" to their job. The problem of individuals performing questionable acts is heightened and even encouraged if the informal ethical code is supported by the excuse that "everyone around them is doing it." Several business ethics studies have found that pressure from subordinates and peers within organizations cause some people to behave unethically (Pierce and Henry, 1996:427).

"The widespread use of computer technology in the workplace affords employees opportunities to perform unethical actions" (Pierce and Henry, 1996:435). "The presence of information technology makes it easier to lie, cheat, steal, vandalize, and violate other commonly accepted ethical rules" (Resnik, 1996:19). "If you shouldn't do something in a face-to-face encounter then don't do it on a network" (Resnik, 1996:19). These concerns may come into play for computer users regardless of whether they are on a personal account at home or on a network at their work site. This is even more critical in a networked society where "everyone around you" can be people they interact with on the network yet never interact with face-to-face. The media is filled with stories of people meeting "kindred spirits" or "soul mates" on the network in chat rooms or through bulletin boards. These faceless, nameless, people manifested anonymously over a coaxial or fiber optic cable can and do share ideas and feelings that may not shared by people in their physical surroundings. This situation may lead to encouragement for unethical behavior that would not normally be performed. An organization cannot afford to depend on each employee's personal code to not perform unethical activities over the organization's network, or even while representing the company on a personal account. Organizations must specify the rules up front, before users begin using the system (Johnson, 1997:65).

Ethical Issues Regarding Network Usage

In 1968, Licklider and Taylor, research directors for the Department of Defense Advanced Research Projects Agency (ARPA), predicted that "in a few years, men will be able to communicate more effectively through a machine than face-to-face" (Boudourides, 1995). Information technology has advanced rapidly in the thirty years since this prediction. In a traditional work environment, typically well defined standards of behavior have been established for decades—in the fields of law and medicine, centuries. However, the area of information technology pertaining to data communications networks is ethically uncharted (Weiland, 1996).

Ethical concerns regarding the capabilities of networking technologies include information privacy, information accuracy, property or ownership of information, and accessibility of information. These issues were identified by Richard Mason in the 1980s and coined with the acronym PAPA (Mason, 1986:5). In addition, there is increasing concern regarding the capability of crime and abuse that can be performed on computer networks. This concern encompasses the responsibility, accountability, and liability of individual users and the organizations that own and maintain networks. Each of these concerns builds on the other due to the unique networking characteristics that enable actions not previously available with traditional technologies. These ethical concerns have been addressed previously regarding advances in technology including railroads, automobiles, radios, and telephones. No previous technology, however, offers the unique combination of capabilities provided by networking technology (Johnson, 1997; Pierce and Henry, 1996; Resnik, 1996). The use of computers adds a new twist to some of these issues as computers are capable of structuring or expediting activities and relationships that existed without them (Johnson, 1994:vii).

Privacy. The most visible ethical concern in the workplace today is privacy (Loch and Conger, 1996:75). Information privacy is defined as "the ability of the individual to personally control information about oneself" (Smith, 1996:168). Individual control over disclosure and use of personal information includes the collection, accuracy and use of that information (Loch and Conger, 1996:75). Concerns about privacy have existed for many years, according to Johnson; "Our society, and western societies generally, have struggled with the issues of privacy for centuries" (Johnson, 1994:vii). These concerns often emerge when the public perceives a threat from the development of new technologies with enhanced capabilities for surveillance, storage, retrieval, and communication of personal information (Culnan, 1993:343). Unique aspects of networking technology have heightened the issues surrounding an individual's privacy regarding personal information and the measurement and performance of work through employee monitoring.

As far back as the turn of the twentieth century concerns regarding privacy were raised. In 1890, the advent of "instantaneous" newsprint and photography prompted Supreme Court justices Warren and Brandeis to advocate the "need to secure for the individual the right to be left alone" (Culnan, 1993:343; Johnson, 1994:90). By the 1970s newly developed computerized systems and automated record-keeping systems led to the enactment of legislation to provide privacy protection (Culnan, 1993:344). The Fair Credit Reporting Act of 1970 provided privacy protection for consumer credit reports and the Privacy Act of 1974 defined citizens' rights and government responsibility for records maintained by the federal government (Johnson, 1994:95). In an attempt to create a validated instrument for measuring individual concern of organizational information privacy practices, Smith concludes there are seven dimensions to such concerns (Smith, 1996:169). These include the collection of personal information, the internal unauthorized secondary use of personal information, the external unauthorized secondary use of personal information, errors in personal information, improper access to personal information, reduced judgment, and the combination of data from different databases which could lead to a *mosaic effect* of individual profiles (Smith, 1996:172). Computer networks are capable of manipulating information on a scale never before anticipated—information can be stored endlessly, sorted efficiently, and located effortlessly (Moor, 1997:27). These capabilities enable information to be retrieved quickly and conveniently, but when speed and convenience lead to the improper disclosure of information in any of the above mentioned dimensions, privacy becomes a far-reaching concern (Moor, 1997:27).

In addition to the traditional issue of an individual's (or an organization's) information privacy, network technology has also emphasized the issue of employee monitoring. In the private sector managers are increasingly using new surveillance technology to monitor and control worker behavior (Linowes, 1993:638). Traditionally employees were monitored directly by supervisors. Today computer monitoring can take the form of monitoring phone calls, timing calls, listening in on private calls, measurement of keystrokes performed by employees, and accessing computer files and electronic mail (e-mail) messages. In most organizations, however, employees expect that a conversation in an office with the door closed is private; that a letter in a sealed envelope will not be opened by others; and that telephone conversations will not be monitored without prior notice (Weisband and Reinig, 1995:40). Networking technology changes these traditional perceptions about private communications in the workplace.

Unlike telephone calls, e-mail messages are treated as documents that, once retrieved, can be used as legal evidence (Weisband and Reinig, 1995:42). Sending an e-mail, posting to a networked bulletin board, or even accessing a World Wide Web page, could be compared to sending a document on official organizational letterhead. In a traditional work environment, once an individual rips up and discards a hard copy document, that particular copy of the document is gone forever. In a networked environment, users may expect the same result when they use the delete key to discard a document. Deleted documents, however, may be archived and stored for many years (Sipior and Ward, 1995:50). In addition, simply because the originator or current owner of that message may destroy the copy or copies available to him or her, that does not mean the document doesn't exist in another location or locations. In online communication, documents may be available to those who manage or monitor the network, unauthorized users, or others who can copy and send them to others ad infinitum (Johnson, 1997:62). "It's no good trying to delete embarrassing e-mail statements because someone will probably have a backup copy of what you wrote" (Forester and Morrison, 1995:5)

Notable uses of e-mail as legal evidence include the Iran-Contra investigations by Congress during 1980s and the case of the Los Angeles police brutality of Rodney King in the 1990s (Sipior and Ward, 1995:50; Weisband and Reinig, 1995:41). In the Iran-Contra investigations deleted e-mail correspondence between Oliver North, John Pointdexter, and other collaborators in the illegal sale of arms to Iran and the illegal transmission of aid to the Contras in Nicaragua were retrieved from an IBM local area network known as PROFS (Professional Office Systems Network) (Forester and Morrison, 1995:48). Oliver North testified before the United States Senate that: "We all sincerely believed that when we sent a PROFS message to another party and punched the button 'delete' that it was gone forever. Wow, were we wrong" (Sipior and Ward, 1995:50). In the King case, Los Angeles police officer Laurence Powell sent an e-mail message to a friend which read: "I haven't beaten anybody this bad in a long time" (Weisband and Reinig, 1995:41). Powell must not have realized that e-mail messages, particularly those composed and forwarded from the workplace, are subject to monitoring by the organization.

Computerized monitoring is constant, reliable, and cheap—supervisors are no longer limited by what they can physically observe with their own eyes (Forester and Morrison, 1995:211). Proponents of monitoring claim it enhances productivity and efficiency while protecting organizations from industrial espionage and the prevention of personal use or abuse of organizational resources (Forester and Morrison, 1995:211; Sipior and Ward, 1995:48). Critics argue that monitoring creates an "atmosphere of suspicion and recrimination resulting in decreased productivity and unacceptable levels of stress" (Rosenberg, 1997:356). Courts have upheld right-to-monitor policies for organizations. Unfortunately, secondary effects of monitoring include increased distrust between managers and employees which in turn leads to lower morale and work productivity (Weisband and Reinig, 1995:42). A 1996 decision by the United States District Court for the Eastern District of Pennsylvania is particularly applicable to the USAF regarding the privacy of government network users. In this decision the judge stated that "the company's interest in preventing inappropriate and unprofessional comments or even illegal activity over its e-mail system outweighs any privacy interest the employee may have in those comments" (Rosenberg, 1997, 305). This case can serve as an example to the USAF because it is also in the best interest of the USAF to ensure information transmitted over computer networks does not compromise the mission of the USAF, the safety of its members, or national security.

Accuracy. Accuracy of information has always been an issue in the workplace; however, this issue has even greater potentially damaging implications due to the tremendous power of information networks. As Mason put it, "misinformation has a way of fouling up people's lives, especially when the party with the inaccurate information has an advantage in power and authority" (Mason, 1986:7). The evolution of networked environments has brought about many issues including accountability, responsibility, integrity, and potential liabilities. Richard Mason believes "a special burden is placed on the accuracy of information when people rely on it for matters of life and death, as we increasingly do" (Mason, 1986:8). Responsibility for accurate information is especially important in a networked environment, because information can be duplicated and transmitted many times over with little effort. Many examples exist which illustrate the consequences of inaccurate information being proliferated by computer technology. A few of these examples are provided by Forester and Morrison: a man mistakenly spent two years in a Los Angeles County jail due to improper use of an automated fingerprint system; another man was arrested, extradited, and confined to a mental facility for 17 months despite available mug shots and fingerprints proving his innocence, and Sheila Jackson Stossier was arrested and jailed due to a National Crime Information Center (NCIC) database match on a warrant for a Shirley Jackson (Forester and Morrison, 1995: 137).

The issue of inaccurate information has potentially significant ramifications for both private and public organizations. In many environments inaccurate information can lead to employee inconvenience and loss of profits and reputation. This problem is magnified exponentially if the inaccurate information is forwarded over a network to others who in turn forward the information or post the information in a common location where users can access the information and pass it on as truth. In 1995 the Microsoft Corporation experienced the consequences of the proliferation of inaccurate information. In this case, a story was disseminated over the Internet that looked like an Associated Press Wire Service article (Basso, 1997:30). The story entailed a fictitious deal between the Vatican and Microsoft in which Microsoft would purchase the Roman Catholic Church for an unspecified number of Microsoft shares (Basso, 1997:30). Although common sense would lead most people to ascertain that this story was a hoax, Microsoft was flooded by calls of those wanting to know if the story was true (Basso, 1997:30). Microsoft was forced to act by issuing formal denials of such a deal through its public relations office (Basso, 1997:30). In the military community inaccurate information can literally mean the difference between life and death. A recent example of the consequences of inaccurate information is the downing of the US Black Hawk helicopters over northern Iraq, killing 26 people in April 1994 (Neumann, 1995:35). Although many factors led to this tragedy, the computer systems in place to identify whether an aircraft was friend or foe provided inaccurate information with which to properly identify the US helicopters (Neumann, 1995:35).

A key issue in each of the examples cited above is how to trace the root of the problem to fix the problem. Tracking the root of the problem encompasses the concepts of accountability, responsibility, integrity and liability. This issue is critical because in cases such as these, society looks for someone to blame—not something, like a computer, but someone—a human being. The excuse that "the computer malfunctioned" or "that's what the computer said" may be inconvenient but not intolerable if someone dials an individual's home phone, because the computer at directory assistance said that was the number to the pizza place. This same excuse is unacceptable if loss of life or components of national security are jeopardized.

Property. The notion of property is closely tied to both privacy and accuracy. This category encompasses the ownership of information—intellectual property and ownership of computer resources—typically by the employer or organization (Loch and Conger, 1996:7). Traditional legal mechanisms currently in place to protect property include copyright, trade secrecy, and patent law (Johnson, 1994:61). These mechanisms, however, were enacted primarily to deal with physical property. The enhanced capability of data communications networks regarding information reproducibility and transmission is now an additional concern to the issues of property and ownership. The issue of who owns information in an electronic form is a relatively new concept. Traditionally, to claim ownership of information, a physical object, such as a book, is needed to serve as a means for the expression of the information (Barlow, 1991:19). Cyberspace removes the physical means leaving only the ideas behind—for "physical manifestations cannot exist in a world where there can be none" (Barlow, 1991:19).

Individual, original items of information can be extremely costly to initially produce. However, once in existence the information has the illusive quality of being easy to reproduce and share with others (Mason, 1986:9). In addition, unlike tangible, physical property, electronic information becomes communicable and difficult to track (Mason, 1986:9). Duplication of the information can take place while keeping the original information intact. Software piracy is an example of this. Software piracy has been a visible issue since its introduction to the workplace. Now that systems are networked together all over the world, however, it is possible for someone outside an organization to copy software and information without authorization and, even more significantly, without the organization knowing the information has been taken.

For the USAF, information on USAF networks belongs to the federal government. Users must not distribute this property over a network without proper authorization. The fact that networks make information easier to access requires that users must be responsible in the information they attempt to access as well as diligent in their efforts to protect the information from those unauthorized to access that information. Users must also ensure that ease of reproducibility does not hurt the integrity of the information. Network users must ensure the data they communicate in the course of their duties is accurate and not compromised in any way.

The abilities to store and transparently transmit large quantities of information over network connections have raised concerns regarding the integrity of available information and the security of sensitive information. When information is duplicated many times over without the originator or recipient knowing where it has been or who has edited it during its journey, one cannot assure the information is correct. In addition, sensitive information, whether personal in nature or that which pertains to government business, can be transparently accessed by unauthorized individuals. Damage resulting from this type of unauthorized action can range from someone learning another person's phone number or bank balance to espionage and the compromise of national security information.

Accessibility. This ethical issue is identified as one of great importance. However, in terms of this research a detailed discussion is beyond the scope of the subject. This section will therefore provide only a brief overview of this issue. The cost and availability of computer technology have decreased considerably in the last decade. Mason notes that this trend has "made technology more accessible and economically attainable to more people; however, corporations and other public and private organizations have benefited the most from these economies" (Mason, 1986:10). He believes that as a result, computation opportunities are primarily available to the middle and upper income people (Mason, 1986:10). This situation brings in a discussion of the haves and the have-nots: those who cannot or choose not to pay for the privilege to access computer databases and networks "are excluded from participating fully in our society" (Mason, 1986:10). This imbalance of accessibility will ultimately lead to many problems in our society because "a just society is one in which benefits and burdens are fairly distributed and all individuals have access to opportunities to achieve their ends" (Johnson, 1994:150).

Computer Abuse and Misuse. Computer actions against organizations include offenses committed by authorized internal users or insiders and those committed by those outside the organization or outsiders (Baase, 1997:230). According to Straub and Nance, computer abuse is "the unauthorized, deliberate, internally recognizable misuse of assets of local organizational information systems by individuals" (Straub and Nance, 1990:47). Abuse can take many forms in a networked environment. Abuse can include the theft or physical damage to hardware, theft or modification of software or data, or the unauthorized use of a computer network. Deborah Johnson breaks abuse out into hacking, software piracy, viruses and worms, intentional versus unintentional abuse, and abuse for fun versus abuse for personal gain (Johnson, 1994:110).

It is critical for an organization as an entity to deal with issues of abuse immediately. An organization's management must know whether members of its workforce knowingly practice unethical behavior on the organization's computer system. It must also know if employees are inadvertently performing improper actions. In 1990 David Paradice recognized this issue which is particularly applicable in today's USAF:

> Although unethical behavior by corporate executives makes headlines, the misjudgments of lower-level staff may ultimately cost organizations more. Errors in judgment may not be spectacular, but they require managerial time and effort to correct. When an employee mishandles a client, uses bad judgment regarding confidential information, or acts in any other manner that reflects poorly on the organization, someone in a senior position must usually take corrective action. In some cases, the employee may not even realize that the actions are unacceptable. In cases where an employee must be dismissed, the

> organization loses its investment in training that employee. (Paradice, 1990:143).

In addition, if unethical acts are practiced on the organization's system, then the organization could be held legally liable for those actions (Rose, 1995:152).

Organizational Perspectives

Traditionally professional organizations such as the Association for Computing Machinery (ACM) and the Institute of Electrical and Electronics Engineers (IEEE) have provided the direction in the area of computing ethics (Pierce and Henry, 1996:426). However, computer usage is much more widespread now than in the past and many who are considered information workers do not belong to or are not closely affiliated with such professional organizations. According to Pierce and Henry, ethical decisions related to computer use are subject to three primary influences: an individual's personal code, an informal code of ethical behavior (peer pressure), and exposure to formal codes of ethics (Pierce and Henry, 1996:425). These three influences seem reasonable not just for computer use but for any action taken by individuals.

These influences would have been exhibited in traditional organizations by physical boundaries; most people would not look at other peoples' mail, go through someone else's desk or office, or make personal phone calls because the records could trace it back to the person. In the current cyber-environment traditional physical boundaries do not exist. Pierce and Henry found that most organizations do not provide the structured framework needed to guide employee behavior regarding computer technology (Pierce and Henry, 1996:425). Of primary concern for organizations is that individuals who do not follow an appropriate ethical code may not only personally perform unethical acts, but can drastically impact the organization by exposing it to possible legal prosecution (Pierce and Henry, 1996:427). Even if legal issues are not involved, acquiring a negative reputation could decimate an organization's reputation or customer base.

The Military Perspective

Computer technology has been integrated into the fabric of the world in a relatively short period of time (Johnson, 1994:150). The developments of networking, in particular, have enhanced communications capabilities in ways never before possible. Unfortunately, along with the benefits of networking, disadvantages have also developed. Of particular concern to the USAF is the misuse of these networks that would bring discredit on the service. Potential ramifications of computer abuse can be expensive in terms of both human and financial resources. Valued employees may be demoted, fired, or resign and the organization may be sued for damages (Henry and Pierce, 1994:21). In the case of the USAF, employees may also be prosecuted and imprisoned for inappropriate use of computers and computer networks. The USAF must ensure measures are in place to protect itself as an organization and its employees from defamation, crime, harassment, and the waste of resources such as man-hours and network usage. The USAF has addressed the ethical issues that have arisen from the expansion of networking by publishing policy directives and USAF Instructions (AFIs).

Lt Col Frank McGovern, Chief of the Air Force communications and information policy at the Pentagon believes "if used properly, e-mail is a superb tool to complement and improve our communications; however, just like other forms of communication, such as the telephone or correspondence, there is a potential for abuse" (Air Force News Service, 1997). The Department of Defense (DoD) has recognized the potential for abuse in the use of networking including the use of Internet and e-mail. In October 1997 the Office of the Assistant Secretary of Defense distributed a memorandum addressing the use of DoD Information and Telecommunications Systems. This memorandum recognizes the importance of the online environment:

> As personal computers, e-mail, and Internet access become ever more ubiquitous, consistent guidance is needed to ensure effective and efficient use of DoD information and telecommunications systems and equipment that are not integral to a weapon or weapon system. (Paige, 1997)

This memorandum also recognized the growing base of insiders or authorized users who were not actual DoD employees but contractors. The recommendation was to ensure the user identification codes and e-mail addresses of contractors were not within the .mil domain. This provision specifically targets the issue of anonymity in networked systems to ensure military members know who they are doing business with and more importantly, identify the member to the recipient of the information.

In the last few years, perhaps in response to the cases cited above, perhaps due to recognition of the fact that "e-mail is becoming a universal method of communication," the DoD and USAF began putting together directives concerning the appropriate use of government sponsored computer networks (Paige, 1997). One thing the departments did not do is take access to networks away from employees or limit network usage to strictly official business where any type of unofficial business would be a cause for disciplinary action. There is allowance for a middle ground as previously discussed. In March 1996 DoD Regulation 5500.7, the Joint Ethics Regulation, was updated to include guidance regarding the use of "e-mail and Internet systems, telephones, facsimile machines and other communications systems and equipment, as well as personal computers, workstations, and other information systems and equipment" (Paige, 1997).

According to paragraph 2-301 of DoD 5500.7-R:

> Federal Government communication systems and equipment (including Government owned telephones, facsimile machines, electronic mail, interact systems, and commercial systems when use is paid for by the Federal Government) shall be for official use and authorized purposes only. (DoD, 1996)

In this case official use includes "emergency communications and communications that the DoD component determines are necessary in the interest of the Federal Government" (DoD, 1996). According to the regulation, authorized usage aside from strictly official business include:

> brief communications made by DoD employees while traveling on Government business to notify family members of official transportation or schedule changes. They also include personal communications from the DoD employee's usual work place that are most reasonably made while at the work place (such as checking in with spouse or minor children; scheduling doctor and auto or home repair appointments, brief Internet searches, e-mailing directions to visiting relatives) when the Agency Designee permits categories of communications, determining that such communications:
>
> (a) Do not adversely affect the performance of official duties by the DoD employee or organization;
>
> (b) Are of reasonable duration and frequency, and whenever possible, made during the DoD employee's personal time such as after duty hours or lunch periods;

> (c) Serve a legitimate public interest (such as keeping DoD employees at their desks rather than requiring the use of commercial systems; educating the DoD employee on the use of communications system; improving the morale of DoD employees stationed for extended periods away from home; enhancing the professional skills of the DoD employee; job searching in response to Federal Government downsizing);
>
> (d) Do not put Federal Government communications systems to uses that would reflect adversely on DoD or the DoD Component (such as uses involving pornography; chain letters; unofficial advertising, soliciting or selling except on authorized bulletin boards established for such use; violations of statute or regulation; inappropriately handled classified information; and other uses that are incompatible with public service; and
>
> (e) Do not overburden the communication system (such as may be the case with broadcasts and group mailings), create no significant additional cost to DoD or the DoD Component, and in the case of long distance communications, charges are:
>
> > 1. Charged to the DoD employee's home telephone number or other non -Federal Government number (third party call);
> >
> > 2. Made to a toll-free number;
> >
> > 3. Reversed to the called party if a non-Federal Government number (collect call);
> >
> > 4. Charged to a personal credit card; or
> >
> > 5. Otherwise reimbursed to DoD or the DoD Component in accordance with established collection procedures. (DoD 1996)

The regulation also addresses the employee monitoring of federal systems with the understanding that "such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized" (DoD, 1996). It also addresses the lack of anonymity when using federal systems because the name, location searched, and computer address of each DoD user is recorded by the government.

Of great importance to the DoD is the protection of classified information. This regulation alerts users that most federal government communications systems are not secure and warns DoD employees not to transmit classified information over any but a secure system. The regulation informs users that DoD employees should exercise extreme care when transmitting sensitive information, or other valued data. It addresses the issues of reproducibility and accessibility as follows:

> Information transmitted over an open network (such as through unsecured e-mail, the Internet, or telephone) may be accessible to anyone else on the network. Information transmitted through the Internet or by e-mail, for example, is accessible to anyone in the chain of delivery. Internet information and e-mail messages may be re-sent to others by anyone in the chain. (DoD, 1996)

This regulation serves as example for the USAF directives involving the use of computers and computer networks. Much of the information, including the phrasing, is the same. Therefore, only significant differences from the DoD 5500.7-R will be discussed further.

USAF Network Specific Directives

AFI 33-119 *Electronic Mail (E-Mail) Management and Use* 1 Mar 97.

According to this AFI, "Air Force e-mail systems are provided to support Air Force missions; only use e-mail systems for official, authorized and ethical activities that are in the best interest of the Air Force." This AFI addresses the ethical issues discussed above as well as the unique features of networking. In regards to privacy, the AFI clearly states that use of any USAF system automatically consents to monitoring; however, "Under no circumstance will monitoring include reading individual e-mail messages without written direction by the commander or local law enforcement officials" (3). The policy also calls for e-mail administrators to "ensure the confidentiality of e-mail viewed in the performance of their duties" (2.6.5).

Accuracy is addressed by the direction to verify the authenticity of messages received (2.7.7) and placing the burden on the receiver to validate taskings received by e-mail (3.2.2). The issue of property is addressed by recognizing e-mail as an official communication (3.1) and discusses information that constitutes an official record and its proper disposition according to records management directives (2.7.3). Accessibility is discussed by instructions to obtain approval before participating in listservers or newsgroups not associated with the USAF. "This policy recognizes that listservers are a potentially valuable information tool for e-mail users; however, the potential for abuse is high" (2.7.5).

Anonymity in this AFI is dealt with in paragraph 2.7.4; "Make sure the account from which the e-mail message was sent is clearly identified. E-mail users will not use anonymous accounts or forwarding mechanisms that purposely attempt to conceal the originator of a message unless approved by the commander for the purposes of soliciting anonymous feedback" (2.7.4). According to this directive, a user is solely responsible for message content of any message he or she transmits and is solely responsible for any material accessed over that network (3.1). Paragraph 8.1.8 cautions users to "be professional and careful..." and to understand that e-mail is easily forwarded; and that messages that are intended to be private or personal may not remain so. Material sent via e-mail is not confidential and is subject to monitoring and retransmittal."

Paragraph 3.5 of this AFI spells out acceptable and unacceptable use of USAF e-mail systems. Authorized uses of these systems are identical to those in DoD 5500.7-R, further noting that the "basic standards for using e-mail are common sense, common decency, and civility applied to the electronic communications environment. This includes following traditional military protocols and courtesies" (3.5.2). The AFI goes a step further than the DoD 5500.7-R by listing unacceptable uses of USAF e-mail systems.

Property and reproducibility are addressed by not allowing users to attach to messages, or otherwise distribute, copyrighted materials without prior consent. "Failure to maintain consent may violate federal copyright infringement laws that could subject the individual to civil liability or criminal prosecution" (3.5.3.1). Misuse of property is addressed in each of these unacceptable acts, especially by forbidding the "transmittal or receipt of e-mail for commercial or personal financial gain using Air Force systems" (3.5.3.2). Other unacceptable actions dealing with privacy and anonymity include "intentionally or unlawfully misrepresenting your identity or affiliation in e-mail communications" (3.5.3.3); "using someone else's identity (userID) and password without proper authority" (3.5.3.5); and "sending harassing, intimidating, abusive, or offensive material to or about others that violates Air Force standards of behavior. This includes but is not limited to humor considered in poor taste or offensive, political or religious lobbying, and pornographic material" (3.5.3.4).

AFI 33-129 *Transmission of Information via the Internet* 1 Jan 97.

This instruction applies to all USAF personnel and "their use of public Internet and web technology such as web servers, web browsers, and file transfer protocol software purchased and licensed by the USAF." Paragraph one of AFI 33-129:

> defines the roles and responsibilities of personnel using and maintaining Internet access. It outlines responsibilities and procedures for accessing information and properly establishing, reviewing, posting, and maintaining government information on the Internet. It also covers responsibilities and procedures for sending e-mail across the Internet. (1)

Paragraph two of this instruction states that "the Air Force goal for the Internet is to provide maximum availability at acceptable risk levels for Air Force members needing access for the execution of official business" (2). The phrasing of this instruction is similar to both the Joint Ethics Regulation (JER) and AFI 33-119 discussed above. This includes a provision under paragraph three, Roles and Responsibilities, which calls for "Commanders and Supervisors to authorize only legal and ethical use of the Internet that is in the best interest of the Air Force" (3.6.2). Stipulations listed for use of personal e-mail authorization are the same as in the JER and AFI 33-119.

Under this instruction, ethical issues of accuracy, property of information, responsibility, and accountability are addressed in part by paragraph three which states that user responsibilities include to:

> Use government equipment and access to the Internet only for official business or authorized activities. Determine the sensitivity and apply appropriate protection to all information transmitted using the Internet. Adhere to copyright restrictions. Protect passwords and access codes. Ensure that all official recorded created while using the Internet are placed in the official records management system. (3.10)

In addition to e-mail, those providing information to Web sites, or Information Providers, are responsible for ensuring material is properly reviewed, cleared, and documented for release on the Internet by the releasing authority (3.11). Documentation is important. Without the documentation the Information Provider as an individual may be accountable for any information which is out on the Internet that should not be. If the documentation shows that the information was officially approved, then the liability shifts to the USAF as an organization. In addition, Information Providers must also ensure the validity of all material available through the Web page.

Government computers are recognized as government property in paragraph six of this instruction, "accessing the Internet through a government computer or network uses a government resource" (6.1). Although this paragraph states that "government-provided hardware and software are for conducting official and authorized government business" this restriction

> does not prohibit commanders from authorizing personnel to use government resources to further their professional and military knowledge if they determine it is in the best interest of the government and authorization is documented by letter, local operating instructions, or explicit policy. (6.1)

Specific prohibitions are listed in paragraph six that are similar to those in the JER and AFI 33-119. One additional prohibition in the offensive material listing includes "hate literature, such as racist literature, materials or symbols, for example swastikas or neo-Nazi materials" (6.1.3). In addition to the prohibition of storing or processing copyrighted material includes a prohibition of using cartoons (6.1.5).

Paragraph eight has specific guidance regarding hypertext references or pointers in World Wide Web pages. The guidance states that pages should "refrain from having pointers on public access pages that reference information outside the functional area of the OPR... In most cases, home pages should point only to parent commands and/or subordinate units" (8.2.1.1). In addition, "pointers to commercial organizations or associations are inappropriate as some may construe them as advertisements or endorsements" (8.2.1.1). For limited access pages (military domain only) "Pointers may point to commercial organizations only if the information is necessary to the performance of official duties" (8.2.1.2).

Paragraph 10 discusses monitoring by stating that organizations can "configure systems so that the system administrator can audit both incoming and outgoing user activities" (10.2). However, the instruction also recognizes that the "monitoring of communications circuits alone will not prevent misuse" and that organizations must "keep misuse of computer systems to a minimum by training and educating personnel on proper uses of the Internet and monitoring their activity" (10.2).

Conclusion

A review of Department of Defense and USAF publications indicates that a majority of the ethical issues identified in the professional and academic literature have been addressed within the guidance for military members. The third and final leg of this research includes the results from a survey of USAF members regarding their opinions of the ethical issues surrounding computers and networking. Chapter III describes the methodology used. Chapter IV describes responses to the survey in detail.

III. Methodology

Introduction

Use of network technology in the USAF is in the relatively early stages. Computer ethics is new enough to the service that there is only one published study in this area—in 1988 an AFIT study was conducted that looked at the status of computer ethics instruction in the USAF (Nelson, 1988). In the academic community, however, there is a significant amount of refereed and professional literature to provide a basis for an introductory study regarding the ethical usage of computers, specifically networks, in the USAF. To gain a preliminary understanding of the use of networks by USAF personnel, a descriptive study was performed to ascertain whether the cases cited in Chapter II are representative of a usage pattern or whether they are simply "growing pains" of the initial stages of network technology. To determine this understanding, an exploratory survey was designed to answer the research questions presented in Chapter I. According to Cooper and Emory, "the area of investigation may be so new or vague that a researcher needs to do an exploration just to learn something about the problem" (Cooper and Emory, 1995: 118). By this definition the use of an exploratory survey is justified for the area of ethical computer usage in the USAF. The results of this survey can be used, in part, to determine whether a more formal study should be performed regarding the appropriate usage of computer networks in the USAF: "Exploratory studies tend toward loose structures with the objective of discovering future research tasks. The immediate purpose of exploration is usually to develop hypotheses or questions for further research" (Cooper and Emory, 1995: 115).

Data Collection Method

This study looked at the area of appropriate network usage from three perspectives. These perspectives include identifying any unique capabilities of computer networks and the corresponding ethical issues regarding a networked environment as well as what DoD and the USAF has provided to users regarding computer and network usage. Finally, the survey will gather responses about how USAF network users view features of a networked environment. Secondary data analysis of professional and academic literature was performed to answer the research questions of what unique capabilities information networks possess and the corresponding ethical issues. Secondary data in the form of DoD regulations and Air Force Instructions (AFI) were examined to determine the USAF's stance on computer and network usage. Finally, an exploratory survey was designed to determine USAF member views regarding the ethical issues of a networked environment.

The survey, approved by the Air Force Personnel Center at Randolph Air Force Base, Texas (USAF SCN: 98-12), was designed to gain an idea of USAF member attitudes regarding the capabilities of computer networks. The survey was comprised of three sections. Part I consisted of eight questions soliciting background demographic data from participants. Part II consisted of eight questions concerning the respondent's background with respect to personal network experience. Finally, Part III consisted of eight scenarios that provided sample situations where identified ethical issues were involved. Participants then answered questions concerning the scenario by rating the their opinions to different uses of network features on a five-point Likert scale. Chapter IV presents the results and discussion of the survey. A copy of the survey is included at Appendix A.

Population and Sample Size

According to Cooper and Emory, a population is a total collection of subjects about which to make some inferences (Cooper and Emory, 1995:200). The relevant population for this study is USAF members who use USAF computer networks. In today's Air Force, use of a network is typically required to gain access to Air Force Instructions, forms, policies, and assignment listings. To control for standardized usage policies and network access, a sampling frame of USAF members on Wright-Patterson Air Force Base (WPAFB) OH was used. Due to the mission and organizations on WPAFB it was expected that a majority of the USAF members assigned to WPAFB would have some experience with network access. Two hundred USAF members were randomly selected from the WPAFB locator maintained by the Aeronautical Systems Center (ASC), the host unit for WPAFB. The surveys were delivered to the unit orderly rooms of each member selected and returned via the WPAFB distribution system.

Data Analysis

Data analysis from this survey is descriptive. The data collected from the secondary data and the survey are not intended as confirmatory data analysis (Cooper and Emory, 1995:393). Instead, the data provide a preliminary overview of the ethical issues the USAF must address as well as USAF member perceptions of and reactions to actions performed in a networked environment. A summary of the data is reported by percentages and numbers reflecting the responses to survey questions. In addition, three categories of the background demographic section (Part I) of the survey were selected to perform limited exploratory data analysis to test whether any differences were found within the responses of the groups (Cooper and Emory, 1995:393).

IV. Survey Responses and Analysis

Introduction

This chapter presents the responses from the survey administered to military members on WPAFB. Of 200 surveys sent out, 89 were completed and returned, yielding a response rate of 44.5 percent. The analysis of the survey responses parallels the structure of the survey. Analysis of the survey begins with the responses to the eight background demographics questions of Part I. Next, responses regarding network related data contained in Part II (questions 9-16) are presented. Finally, responses to the eight scenarios provided in Part III are analyzed.

Part I. Responses to Background Demographics

Part I of the survey consisted of eight questions designed to gather background demographic information. Items requested included grade, age, length of employment with the USAF, length of time assigned to present office, level of command at which respondent is located, supervisory and managerial input, and whether respondents considered themselves simply computer users or a computer professional. Discussion and frequency breakouts per question follow.

Question 1. Survey respondents represented every grade indicated on the survey. The highest percentage of respondents fell in the 0-3 to 0-4 range, 35.96 percent with the 0-1 to 0-2 range following at 24.72 percent. The survey, therefore, was completed by a majority of officers in the grades of 2nd Lieutenant through Major—60.7 percent. Respondents in the enlisted grades of Airman Basic (E-1) through Technical Sergeant (E-6) and above comprised 31.5 percent of the responses. The remaining 7.8 percent of the respondents were in the grade of Lieutenant Colonel (0-5) or above. Grade response frequencies and corresponding percentages are displayed in Table 1.

Table 1: What is your grade?

Grade	Frequencies	Percentage
E-1 to E-3	2	2.3
E-4 to E-5	14	15.7
E-6 or above	12	13.5
0-1 to 0-2	22	24.7
0-3 to 0-4	32	36.0
0-5 or above	7	7.8
other	0	0
Total	89	100

Question 2. The largest number of responses fell in the age range of 26 through 30 (30.4 percent) and 31 through 35 (25.8 percent). This percentage of 56.2 in the age groups of 26 through 35 corresponds to the 60.7 percent found in the grades of 0-1 through 0-4. A majority of company grade and junior-level field grade officers belong to both of these groupings. Frequencies and corresponding percentages are shown in Table 2.

Table 2. What is your age group?

Age	Frequencies	Percentage
18 to 25	14	15.7
26 to 30	27	30.4
31 to 35	23	25.8
36 to 40	13	14.6
41 or above	12	13.5
Total	89	100

Question 3. A majority of the respondents had been employed by the USAF for 1 to 5 years (30.3 percent). The frequencies indicate a slightly larger proportion, 55 percent of the respondents, were employed by the USAF for 10 years or less. Respondents employed by the USAF for 11 or more years had a frequency rate corresponding to 45 percent. Responses and corresponding percentages are shown in Table 3.

Table 3. How long have you been employed by the USAF?

Length of Employment	Frequencies	Percentage
1 to 5 years	27	30.3
6 to 10 years	22	24.7
11 to 15 years	17	19.1
16 to 20 years	21	23.6
More than 20 years	2	2.3
Total	89	100

Question 4. As expected for military personnel, a large percentage of the respondents had been working in their office for less than two years (76.4 percent). To enhance career development, USAF policy encourages officers to take on a new job or assignment every three years. Since the largest percentage of responses were officers in the grades of 0-1 through 0-4 (60.7 percent), it is reasonable that the percentage for

Question 4 is 76.4 percent. Breakouts and percentages for Question 4 are displayed in Table 4.

Table 4. How long have you been working in your present office?

Present office	Frequencies	Percentage
Less than one year	39	43.8
1 to 2 years	29	32.6
More than 2 but less than 5	20	22.5
More than 5 but less than 8	0	0
More than 8 years	1	1.1
Total	89	100

Question 5. Two individuals did not respond to this question. The largest proportion of respondents, 76.4 percent, indicated they worked at the squadron or division level or below. Individuals performing at these levels would typically be workers who must abide by policies set out by upper management. Local management and policy makers typically work at the Wing/Base, Group, or Directorate Level to which 21.4 percent of the respondents belonged. Questions responded to as *other* were typically identified as AFIT students. Responses and percentages are broken out in Table 5.

Table 5. At what level of command is your office located?

Level of Command	Frequencies	Percentage
Wing/Base	9	10.1
Group	5	5.6
Squadron	10	11.2
Flight	3	3.4
Directorate	5	5.6
Division	13	14.6
Branch	22	24.7
Section	8	9.0
Other	12	13.5
Total	87	97.7

Question 6. This question was intended to discover how many of the respondents supervised other individuals. Those individuals who supervise others are in a position to pass on organizational policies regarding network usage and to implement local policies for their areas. The frequency of respondents who indicated they were supervisors is 32.6 percent. Two hundred and forty-five individuals are supervised by these respondents. Frequency breakouts and percentages are located in Table 6.

Table 6. Do you directly supervise employees?

Supervisor?	Frequencies	Percentage
Yes	29	32.6
No	60	67.4
Total	89	100

Question 7. This question was intended to determine which individuals considered themselves managers. As managers, these individuals would be responsible for passing on and implementing network usage policies. While sorting through the responses, a pattern was observed with Question 7 suggesting there might have been a problem with

the phrasing of the question. If Question 6 was answered yes, then the phrasing of Question 7 may have suggested to not answer Question 7. For this reason another item was added to the results in Table 7 indicating those who did not respond to Question 7. Each of the 18 individuals who did not respond to Question 7 answered yes for Question 6. This would indicate that the total of Yes responses and Didn't Answer responses might be considered managers and/or supervisors—36 respondents or 40.4 percent of the sample. Breakouts and percentages are shown at Table 7.

Table 7. If you do not directly supervise employees are you considered a manager?

Manager?	Frequencies	Percentage
Yes	18	20.2
No	53	59.6
Didn't Answer	18	20.2
Total	89	100

Question 8. This question asked respondents to classify themselves as computer users or computer professionals. A computer user was defined as one who uses computers in the office but does not design or program computers. A computer professional was identified as one who is able to program, design, or configure a computer or computer network. One individual did not respond to this question and one individual identified both classifications. Breakouts and percentages are located at Table 8.

Table 8. Do you consider yourself a computer user or computer professional?

User or Professional?	Frequencies	Percentage
Computer user	62	69.7
Computer professional	26	29.2
Total	88	98.9

Part II. Responses to Network Related Data Questions

Part II of the survey consisted of eight questions designed to gather information regarding the respondents' experience with networks. Items asked: for how long the respondent's office had access to a network, what respondents used network access for, and how often respondents used the available network. In addition, the survey requested an overall perception of the amount of work performed on a network by the individual, a Likert scale of 1-10 asking respondents to rate the effectiveness of networking in enhancing their personal duty performance, and whether the respondent's organization had provided specific guidance regarding appropriate usage of government networks. Finally, Part II asked if the respondents had ever observed or experienced what they believed was inappropriate usage of computers or networks within the workplace. The final question was an open-ended question that asked respondents to describe their experiences if the answer to the previous question was yes. Discussion and frequency breakouts follow discussions for each question.

Question 9. This question provided 6 possible responses (a through f). Twenty-six respondents either did not answer the question or wrote in that the network was in place when they were assigned to that office. This was identified as a problem with the question because respondents were not offered the option to choose that the network be in place when they arrived at their present office. Therefore, for the response breakout in Table 9, an additional item was added for the 19 individuals who noted the network predated them. Responses do not add up to 100 percent because eight individuals did not select any of the choices provided, nor did they volunteer any information on the survey.

Table 9. Approximately how long has your office had access to a network?

Length of Access	Frequencies	Percentage
Less than one year	2	2.3
1 to 2 years	6	6.7
More than 2 but less than 5 years	27	30.3
More than 5 but less than 8 years	14	15.7
More than 10 years	2	2.3
My office does not have access to a network	12	13.5
Network predates respondent	10	21.4
Total	82	92.2

Question 10. This question asked respondents to choose as many as applied. Interestingly, in Question 9, 12 individuals noted they did not have access to a network; however, 100 percent of the respondents said they used at least one form of network application—specifically e-mail. This may indicate that some individuals may not consider an e-mail capability as a networking function. Answers to the open-ended item entitled *other* listed the following:

- “everything”
- Formflo (USAF automated forms program)
- PC III (military personnel system)
- common project data
- research tools
- distance learning
- File Transfer Protocol (FTP)

- databases
- File Saver
- Classified
- Data processing/engineering (Mathcad/MATLAB)
- Shared Drives
- Planning information

Since this list asked respondents to choose as many that apply, the number of responses and the percentage of respondents listing each item in Table 10 do not add up to 100 percent.

Table 10. What do you use your network access for?

Access Used For	Frequencies	Percentage
E-mail	89	100
Organizational bulletin board	39	43.8
Internet/World Wide Web access	86	96.6
Access to organizational documentation	66	74.2
Distribution of documentation	59	66.3
Other	17	19.1

Question 11. Similar to Question 10, although 12 individuals indicated their offices did not have access to a network in Question 9, no individuals responded to the first two items of Question 11. A majority of the respondents, 48.3 percent, used their network throughout the day while 32.6 percent accessed the network several times a day. Only one individual did not respond to this item. Frequency responses and percentages are listed in Table 11.

Table 11. In your present position, how often do you use your office network?

Frequency of Network Use	Frequencies	Percentage
Do not use network	0	0
At least once a month	0	0
At least once a week	1	1.1
At least once a day	15	16.9
Several times each day	29	32.6
Log in upon arrival and work all day	43	48.3
Total	88	98.9

Question 12. In this item the majority of individuals responded that they accomplished either some of their work (48.3 percent) or a majority of their work (37.1 percent) with a network. Two respondents listed two responses. Therefore totals found in Table 12 exceed 100 percent.

Table 12. Do you use the network to accomplish:

Work accomplishment	Frequencies	Percentage
All of your work	8	9.0
A majority of your work	33	37.1
Some of your work	43	48.3
Very little of your work	7	7.9
None of my work	0	0
Total	91	102.3

Question 13. This question asked individuals to rate the effectiveness of networking in their own duty performance. This question was formed as a Likert scale ranging from 1 through 10. Number 1 was ranked as not at all effective with number 10 ranking extremely effective. The scores ranged from a low of 2 to a high of 10.

Table 13. Rate effectiveness of networking in enhancing your duty performance

Effectiveness of networking	Frequencies	Percentage
1	0	0
2	1	1.1
3	1	1.1
4	1	1.1
5	5	5.6
6	3	3.4
7	11	12.4
8	36	41.8
9	18	20.2
10	10	11.2
Overall Average Score	7.63	

Question 14. The goal of this question was to investigate whether respondents believed their organization had provided its members guidance regarding network usage. This question asked for a yes or no response. This question was not intended to measure the effectiveness of the guidance. One person did not respond to this question.

Table 14. Has your organization provided guidance regarding appropriate usage of organizational computer networks?

Guidance regarding use provided	Frequencies	Percentage
Yes	76	85.4
No	12	13.5
Totals	88	98.9

Question 15. This question was intended to gain an understanding of respondent's personal experience with the inappropriate usage of computers and networks in the workplace. This question was followed by an open-ended question asking those who responded that they were aware of inappropriate usage in the workplace to describe their experience.

Table 15. Have you ever observed inappropriate usage in the workplace?

Observed inappropriate use	Frequencies	Percentage
Yes	31	34.8
No	58	65.2
Totals	89	100

Question 16. Question 16 was an open-ended question asking respondents to describe any inappropriate usage they had experienced in the workplace. In Question 15, 31 individuals responded that they had observed some form of inappropriate usage in the workplace. Experiences listed included:

- Accessing dating services during duty hours
- Person in leadership position promoting a specific real estate company on organization's e-mail
- Internet auto purchase search by military member
- E-mailing love letters between coworkers, both married to others
- Personal investments
- Searching Internet for want-ads
- Checking professional game scores over Internet
- Non-mission related Web surfing
- E-mail friends unofficially
- Games
- Personal use of systems
- Net surfing inappropriate sites
- Overuse of personal e-mail
- Unofficial e-mail
- Net surfing
- Prepare/print fliers for off-duty interests
- Loading home software on government system
- Loading government software on personal systems
- Net surfing for "sexually explicit material"
- Games on government computers
- Unofficial Web pages
- Forwarding inappropriate mail, humor
- Excessive use of chat rooms on Internet
- Downloading tax forms
- Unofficial Internet usage
- Inappropriate e-mail and personal Web surfing

Part III. Sample Scenarios

The scenarios provided in the survey were created to gather opinions from military members regarding certain ethical aspects of network usage in the workplace. The scenarios were not intended to gather knowledge of actual USAF policies and procedures regarding computer and network usage. The scenarios, instead, were intended to gauge the respondents' initial reaction to each question regarding the scenario. Questions following each scenario were rated on a Likert scale of 1 (strongly disagree) through 5 (strongly agree). All scenarios were kept as generic as possible indicating no rank or specific location. Each of the scenarios is briefly described below with the frequency rating annotated for each question. All 89 individuals responded to each question and all percentages add to 100 percent. Full scenarios are located within the original survey located at Appendix A.

Scenario 1. This scenario deals with the ethical issues of property, responsibility, accessibility, and reproducibility. Using a network, Jack, a government employee, downloads government software to his personal computer at home. He spends a lot of extra hours working on the project at home. He did not inform anyone at his organization that he downloaded the program at home. His wife discovers the software on the computer and decides to use it for some of her private freelance work. The average ratings noted in Table 16 indicate the respondents did not approve of Jack downloading the software without notifying his organization. The lowest average rating was that of Jack's wife using the software, most respondents noting that it should be used for official government business only. The average ratings indicate that respondents believe, overall, that Jack should not have placed the software on his personal computer.

Table 16. Scenario 1: Question 1a

It is okay that Jack downloaded the software; he had valid reasons

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	20	22.5	2.92
2. Disagree	21	23.6	
3. Neither agree/disagree	8	9.0	
4. Agree	26	29.2	
5. Strongly Agree	14	15.7	

Table 17. Scenario 1: Question 1b

Since Jack is working extra hours he's allowed to download software

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	43	48.3	2.06
2. Disagree	21	23.6	
3. Neither agree/disagree	9	10.1	
4. Agree	9	10.1	
5. Strongly Agree	7	7.9	

Table 18. Scenario 1: Question 1c

No problem with Jack's wife using the software

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	64	71.9	1.42
2. Disagree	18	20.2	
3. Neither agree/disagree	4	4.5	
4. Agree	1	1.1	
5. Strongly Agree	2	2.2	

Table 19. Scenario 1: Question 1d

Since USAF will benefit it's okay if Jack uses the software at home

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	21	23.6	2.89
2. Disagree	18	20.2	
3. Neither agree/disagree	12	13.5	
4. Agree	26	29.2	
5. Strongly Agree	12	13.5	

Scenario 2. Ethical issues encompassed by this scenario are computer abuse (crime), accessibility, privacy, property, accuracy, liability, and anonymity. The scenario describes a situation where Carol uses her government computer to access a private credit bureau system. She does this to help a friend, a fellow government employee,

find out whether her credit rating will reflect badly on her security clearance. Carol did not make any changes to the data in the system she accessed—she simply looked at the information. The average ratings listed in Tables 20 through 23 indicate that the respondents disapproved of Carol's actions. Only 11 out of 89 respondents (12 percent) replied in the agree—strongly agree range that Carol's actions were acceptable. However, 60 percent of the respondents thought that Carol should alert the system administrator of the credit bureau that their system was easily accessible. Seven percent believed Carol should not notify the administrator while 33 percent ranked this item as neither agree nor disagree.

Table 20. Scenario 2: Question 2a

Carol's actions would not be considered wrong.

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	38	42.7	
2. Disagree	32	36.0	2.00
3. Neither agree/disagree	5	5.6	
4. Agree	9	10.1	
5. Strongly Agree	5	5.6	

Table 21. Scenario 2: Question 2b

As long as no changes were made, it's okay for Carol to "browse"

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	49	55.1	1.70
2. Disagree	28	31.5	
3. Neither agree/disagree	5	5.6	
4. Agree	4	4.5	
5. Strongly Agree	3	3.4	

Table 22. Scenario 2: Question 2c

An employee of the bank can appropriately access the system

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	17	19.1	
2. Disagree	13	14.6	2.96
3. Neither agree/disagree	25	28.1	
4. Agree	25	28.1	
5. Strongly Agree	9	10.1	

Table 23. Scenario 2: Question 2d

Carol should alert the system administrator

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	5	5.6	3.71
2. Disagree	1	1.1	
3. Neither agree/disagree	30	33.7	
4. Agree	32	21	
5. Strongly Agree	21	23.6	

Scenario 3. This scenario dealt with the use of government resources to support a personal, for-profit business. In this case, a senior-level manager is starting a business on the side. His partner worked in the personnel office of the same organization. Since they were aware it would be improper to approach people at work to discuss investing in their business, the senior-level manager asks the personnel partner to pull the home phone numbers, addresses, and home e-mail addresses of people they want to contact from the organization's personnel database. The ethical issues of privacy, property, accessibility, computer abuse, and liability are incorporated in this scenario. Average ratings indicate that the respondents did not approve of the actions taken.

Table 24. Scenario 3: Question 3a

Bill's request to Mary was perfectly legitimate

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	51	57.3	1.54
2. Disagree	31	34.8	
3. Neither agree/disagree	5	5.6	
4. Agree	1	1.1	
5. Strongly Agree	1	1.1	

Table 25. Scenario 3: Question 3b

There is no problem with Mary gathering information off the network

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	50	56.2	1.62
2. Disagree	29	32.6	
3. Neither agree/disagree	6	6.7	
4. Agree	2	2.2	
5. Strongly Agree	2	2.2	

Table 26. Scenario 3: Question 3c

It was general information, so it isn't a problem using information

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	53	59.6	1.55
2. Disagree	29	32.6	
3. Neither agree/disagree	2	2.2	
4. Agree	4	4.5	
5. Strongly Agree	1	1.1	

Table 27. Scenario 3: Question 3d

I would have no problem with someone accessing my information

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	54	60.7	1.52
2. Disagree	27	30.3	
3. Neither agree/disagree	6	6.7	
4. Agree	1	1.1	
5. Strongly Agree	1	1.1	

Scenario 4. This scenario deals with issues of property, abuse, liability, and anonymity. A government computer programmer begins a small side business and goes to his office on weekends to work on the network. The average ratings to the responses to the questions indicate overall disagreement with the networking behavior in the

scenario. Response frequencies and average Likert scale ratings for Scenario 4 can found in Tables 28 through 30.

Table 28. Scenario 4: Question 4a

Paul should not have a business on the side

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	55	61.8	1.52
2. Disagree	24	27	
3. Neither agree/disagree	8	9.0	
4. Agree	2	2.2	
5. Strongly Agree	0	0	

Table 29. Scenario 4: Question 4b

Use of the network completely appropriate

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	48	53.9	1.65
2. Disagree	29	32.6	
3. Neither agree/disagree	8	9.0	
4. Agree	2	2.2	
5. Strongly Agree	1	1.1	

Table 30. Scenario 4: Question 4c

Since information did not pertain to government it's okay

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	47	52.8	1.71
2. Disagree	29	32.6	
3. Neither agree/disagree	7	7.9	
4. Agree	2	2.2	
5. Strongly Agree	3	3.4	

Scenario 5. This scenario involves the ethical issues of responsibility, accuracy, liability, accountability, and property of information. In this case, a data entry division has had an upgrade made to the primary entry system. Unfortunately, Cliff was not told of the changes until a sizable amount of data was entered incorrectly. Cliff takes it upon himself to decide to leave the inaccurate data in the system because he does not feel the time and resources needed to update the information would be justified. Respondents seemed to believe the data should have been changed regardless of whose fault it was that the data is now inaccurate. Responses indicate that members feel Cliff has a responsibility to correct the data to ensure accuracy. Several respondents noted the organization could be held accountable or liable for incorrect data obtained from the system. The information is government property and it is Cliff's responsibility to protect the organization from liability due to the distribution of incorrect information.

Response frequencies and average Likert scale ratings for Scenario 5 can found in Tables 31 through 34.

Table 31. Scenario 5: Question 5a

Cliff was right to not "waste" government resources

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	51	57.3	1.57
2. Disagree	29	32.6	
3. Neither agree/disagree	7	7.9	
4. Agree	0	0.0	
5. Strongly Agree	2	2.2	

Table 32. Scenario 5: Question 5b

System designers did a good job designing the new system

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	15	16.9	
2. Disagree	26	29.2	2.57
3. Neither agree/disagree	34	38.2	
4. Agree	10	11.2	
5. Strongly Agree	4	4.5	

Table 33. Scenario 5: Question 5c

Systems administrators can change system whenever they want

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	32	36	1.83
2. Disagree	42	47.2	
3. Neither agree/disagree	14	15.7	
4. Agree	0	0.0	
5. Strongly Agree	1	1.1	

Table 34. Scenario 5: Question 5d

Cliff's actions were appropriate, his boss is at fault

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	36	40.4	1.81
2. Disagree	40	44.9	
3. Neither agree/disagree	9	10.1	
4. Agree	2	2.2	
5. Strongly Agree	2	2.2	

Scenario 6. This scenario describes a government employee who often has extra time during duty hours while waiting for her next assignment. Joanne often browses the Internet to keep herself busy. She accesses government sites to keep updated on her job. However she also routinely accesses current stock exchange information for her

personal portfolio. In this case the ethical issues entail property of government equipment (including online network time), liability, and responsibility.

Average responses from survey participants for all four questions fell in a 2.90 to 3.60 range. This indicates the respondents neither overwhelmingly approved nor disapproved with Joanne's actions. For Question 6a it appeared that the respondents were split three ways as to whether they believed Joanne's use of her extra time was appropriate or not; 24.7 percent answered that they disagreed with Joanne's use of her extra time, 23.6 percent responded they did not agree nor disagree with Joanne's use of her time, and 27 percent indicated that they agreed that Joanne's use of time was appropriate. However, 43.8 percent favor Joanne notifying her boss of her extra time on the job (Question 6c) so he or she can make a decision of what she should do with Joanne's time.

For Question 6b regarding use of limited personal business on an organizational network, responses once again appear to be split between the agree and disagree range with 13.5 percent of the respondents indicating neither agree nor disagree. Eighteen percent strongly disagreed while 28.1 percent disagreed that personal use was appropriate. In the agree range of Question 6b, 32.6 percent agreed and 7.9 percent strongly agreed that limited personal usage was appropriate. Some respondents did note that phone policies usually allow limited personal use if usage is in the best interest of the USAF and does not interfere with official duties. These respondents seemed to treat the usage of USAF networks in a similar manner as phone usage. One individual did not choose to answer Question 6a. Response frequencies, percentages, and average Likert ratings can be found in tables 35 to 38.

Table 35. Scenario 6: Question 6a

Joanne's use of extra time is entirely appropriate

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	12	13.5	
2. Disagree	22	24.7	2.96
3. Neither agree/disagree	21	23.6	
4. Agree	24	27	
5. Strongly Agree	9	10.1	

Table 36. Scenario 6: Question 6b

Joanne can perform limited personal business on network

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	16	18.0	
2. Disagree	25	28.1	2.85
3. Neither agree/disagree	12	13.5	
4. Agree	29	32.6	
5. Strongly Agree	7	7.9	

Table 37. Scenario 6: Question 6c

Joanne should let her boss know of her extra time on the job

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	2	2.2	
2. Disagree	10	11.2	
3. Neither agree/disagree	24	27	3.60
4. Agree	39	43.8	
5. Strongly Agree	14	15.7	

Table 38. Scenario 6: Question 6d

Joanne's use of the phone was entirely inappropriate.

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	8	9.0	
2. Disagree	32	36	2.90
3. Neither agree/disagree	19	21.3	
4. Agree	21	23.6	
5. Strongly Agree	9	10.1	

Scenario 7. This scenario regards a supervisor, Alan, having a friend who is a system administrator access a subordinate's (John) account to see if John had any electronic correspondence with the Command Section. Although none was found, the system administrator did note that there was correspondence regarding John possibly

applying for an opening in another office. Because of the information gleaned from the system administrator, Alan does not consider John for a promotion because he thinks John is leaving his area. This scenario entails the ethical issues of abuse, privacy, property, accessibility, anonymity, accuracy, and liability. The biggest abuse was the misuse of government resources to illegally access another's account while also compromising the employee's privacy and confidentiality. The files accessed were government property and were used to make an official decision without any validity of the accuracy of the information. John's anonymity was compromised because he may not have wanted his supervisor to know he was thinking of moving areas, possibly for the very reason that he knew it would hurt his chances of promotion. Finally, Alan's and the administrator's actions have placed the organization in a position where they are liable for these actions, and could be held responsible for John's not receiving his promotion.

A majority of the responses to Question 7a, claiming Alan was perfectly within his rights to acquire any information on his subordinates he sees fit, fell in the strongly disagree and disagree range, 65.2 and 24.7 percent respectively. Only 9 percent responded they did not agree nor disagree and one individual agreed Alan could act this way. No responses corresponded to strongly agree. In addition, for Question 7b, which states there is nothing wrong with the system administrator auditing John's files because it is part of an administrator's job, responses again clustered in the disagree range with 39.3 percent falling in the strongly disagree area and 19.1 percent falling in the disagree area. 24.7 percent of the respondents answered neither agree nor disagree leaving only 16.8 percent in the agree range of the scale. This same pattern was seen in Questions

7c, regarding John's use of the system regarding a new position not being appropriate, and 7d claiming the system administrator had every right to provide Alan with information outside the realm of which Alan was asking. A majority of responses for these two questions fall in the disagree range, 78.7 and 88.8 percent respectively. For Question 7e regarding John's right to file a complaint against Alan and the administrator, over 70 percent of the responses fell in the agree range. These responses occurred even though the files and the information in them are technically government property. Some individuals answered this question in two parts recognizing that Alan's actions were inappropriate while the system administrator's actions were allowable under certain conditions, such as a court order or Commander's approval. Tables 39 to 43 list frequency breakouts and percentages for Scenario 7.

Table 39. Scenario 7: Question 7a

It is Alan's right to acquire the information he received

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	588	65.2	1.46
2. Disagree	22	24.7	
3. Neither agree/disagree	8	9.0	
4. Agree	1	1.1	
5. Strongly Agree	0	0.0	

Table 40. Scenario 7: Question 7b

Nothing wrong with system administrator auditing John's files

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	35	39.3	
2. Disagree	17	19.1	2.21
3. Neither agree/disagree	22	24.7	
4. Agree	13	14.6	
5. Strongly Agree	2	2.2	

Table 41. Scenario 7: Question 7c

Sending e-mail about a new job in the organization isn't appropriate

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	32	36	1.98
2. Disagree	38	42.7	
3. Neither agree/disagree	11	12.4	
4. Agree	5	5.6	
5. Strongly Agree	3	3.4	

Table 42. Scenario 7: Question 7d

System administrator had every right to provide Alan information

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	51	57.3	1.55
2. Disagree	28	31.5	
3. Neither agree/disagree	9	10.1	
4. Agree	1	1.1	
5. Strongly Agree	0	0.0	

Table 43. Scenario 7: Question 7e

John has a right to file a complaint

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	2	2.2	
2. Disagree	6	6.7	
3. Neither agree/disagree	17	19.1	
4. Agree	27	30.3	4.02
5. Strongly Agree	37	41.6	

Scenario 8. This final scenario dealt with an issue faced in the workplace on a regular basis today. The ethical issues involved in this scenario are property, abuse, accountability, and liability. In this case an administrator in the Commander's office, Robin, is showing a secretary, Karen, how to use the organization's network. Robin

used a new message in her e-mail inbox to show Karen how to access, compose, and reply to electronic mail messages. The message Robin used happened to be a short message from her daughter at college which Robin briefly responded to. Karen later took it upon herself to report her observation of Robin's computer misuse to the Fraud, Waste, and Abuse Office.

In this case responses again seemed to favor the disagree portion of the scale. In Question 8a, stating that Karen had acted appropriately in reporting Robin, 33.7 percent and 34.8 percent answered strongly disagree and disagree respectively. Only 19.1 percent answered neither agree nor disagree while only 12.3 percent responded in either of the agree ratings. A similar pattern was seen in the other questions, in which responses generally fell in the disagree portion of the scale in the questions stating that Robin replying to her daughter's message over the network was inappropriate, that it was Karen's responsibility to report Robin, and that Robin should be disciplined for using the network for personal business. Tables 44 to 47 list the response frequencies and average Likert scale rating for each question.

Table 44. Scenario 8: Question 8a

Karen was acting appropriately in reporting Robin

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	30	33.7	
2. Disagree	31	34.8	2.12
3. Neither agree/disagree	17	19.1	
4. Agree	9	10.1	
5. Strongly Agree	2	2.2	

Table 45. Scenario 8: Question 8b

Robin replying to the message over the network was inappropriate

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	23	25.8	
2. Disagree	38	42.7	2.20
3. Neither agree/disagree	17	19.1	
4. Agree	9	10.1	
5. Strongly Agree	2	2.2	

Table 46. Scenario 8: Question 8c

It was Karen's responsibility to report Robin

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	24	27.0	
2. Disagree	25	28.1	2.40
3. Neither agree/disagree	24	27	
4. Agree	12	13.5	
5. Strongly Agree	4	4.5	

Table 47. Scenario 8: Question 8d

Robin should be disciplined for using the network the way she did

Likert Rating	Frequencies	Percent	Average Likert Rating
1. Strongly Disagree	342	38.2	1.99
2. Disagree	32	36.0	
3. Neither agree/disagree	16	18.0	
4. Agree	4	4.5	
5. Strongly Agree	3	3.4	

A Concurrence of Views

Discussion and data provided above indicated there was considerable consistency between the responses regarding the behavior outlined in the scenarios. To support this indication, the data of three categories in the Part I demographics, *grade*, *age*, and *level of command*, were selected to examine whether there was indeed a concurrence in the views of the respondents, across each of the three areas.

Grade Consistencies. *Grade* was the first category analyzed. Responses to scenario questions by enlisted participants (E-1 to E-6+) were compared with the responses of the officers (0-1 to 0-5+). The objective of comparing these two populations was to investigate whether there was a significant difference between the responses of the two groups. The mean, standard deviation, and differences between the means were calculated for each of the 32 questions in Part III of the survey. The data were then used to test the null hypothesis that responses of the two groups were the same (H_0: M_e=M_0) against the alternative hypothesis that the responses were significantly different (H_A: $M_e < M_0$ or $M_e > M_0$).

A total of 28 enlisted responses were compared against the 61 officer responses. To test the hypotheses a z-statistic was constructed to determine if a significant difference existed between the means of the two groups. This statistic was computed based on a two-tailed test at the .10 level of significance (.05 at each tail) and the assumptions that sampled populations had an approximately normal relative frequency distribution, the sample variances were equal, and the samples were randomly and independently selected from their respective populations.

The p-value calculated for all but one question was greater than the alpha level of .05 for each tail. The one exception was a p-value of -.002 for response S1d. Question d for Scenario 1 stated: "It's okay for Jack to have this software on his home computer because the USAF will benefit." The enlisted mean for this question was 2.82 and for the officers was 3.04. The calculated p-value indicates that the officers seemed more inclined to disagree with the statement. Based on the majority of the p-values, the alternative hypothesis would be rejected at the .01 level of significance. Therefore, overall finding for this scenario suggests that there is little difference in the responses between the enlisted and officer groups. The significance of this conclusion for the USAF is that both the enlisted and commissioned grades concur in their views regarding the ethical behavior in a networked environment. This is important to the USAF because there is a strong likelihood that officers and enlisted personnel will be in a supervisor-subordinate relationship. Concurrence in their views regarding behavior in a networked work environment can reduce conflict that may arise if the two groups have diverging views. The data for this hypothesis test is located at Appendix B.

Age Consistencies. Age was the next category selected from Part I of the survey. This category, which offered respondents five choices on the survey, was divided into two groups. The first group was composed of those in the 18-30 age range and the second group was made up of those respondents in the 31 and over age range. The two groups again were compared to investigate whether there was a difference in responses between those under the age of 31 and those the age of 31 and over. The mean, standard deviation, and differences between the means were again calculated for the responses to each question in Part III of the survey. The hypotheses tested with this data were the same as for the *grade* data—are the responses of the two groups the same (H_0: $M_{-31}=M_{+31}$) or are the responses different (H_A: $M_{-31}<M_{+31}$ or $M_{-31}>M_{+31}$).

A total of 41 respondents were under the age of 31 and 48 of the respondents were age 31 or over. Because the sample sizes were larger than 30 (n>30) a large-sample test of hypothesis for the difference in the means was performed using a z-statistic (McClave and Benson, 1995:393). The calculated z-statistic was based on a .10 level of significance in a two-tailed test and two assumptions. The first assumption is that the two samples were randomly selected in an independent manner from the two populations. The second assumption was that the sample sizes were large enough (>30) that the means of each sample had an approximately normal sampling distribution.

Of the 32 p-values calculated at the .10 level of significance, only four resulted in values of less than .05. These questions were in scenarios three, four, and six. For Scenario 3, question b stated that there is no problem with Mary gathering private information off the organization's network. According to the p-values, the 31+ age group was less inclined to agree with this statement (Mean = 1.38) than the 18-39 age group (Mean =1.90). This finding may be an indication that the younger troops have different ideas regarding privacy of personal data and use of networks than the 31+ age group. Scenario 4 had two p-values which found a significant difference between the groups existed for questions b and c. Question b stated that since network resources would be sitting idle over a weekend then it was okay for Paul to use the network over the weekend for personal business. For this question the 18-30 age group were more likely to agree (Mean = 1.94) with this statement than the 31+ age group (Mean = 1.40). Question c stated that since Paul was gathering non-government information then there is no problem using the network for information in the public domain. The 18-30 age group had a mean of 2.01 for this question whereas the 31+ age group averaged out to 1.46. This difference indicates that there may be potential conflicts regarding how networks may be used when utilized after duty hours. The final p-value indicating a significant difference between the means of the two groups showed that the 18-30 age group had a higher mean (Mean = 3.09) while the 31+ age group were on the lower end of the scale (Mean = 2.65). The question this value referred to was in Scenario 6, question b. This question states that there is nothing wrong with Joanne performing limited personal business over the organization's network as long as it does not interfere with her job. The younger group responded they were more likely to lean towards agreeing with the statement. The 31+ age group, however, seemed more inclined to disagree with the statement.

This finding indicates there is little difference in the responses between the two age groups. This consistency between responses is significant to the USAF because younger members typically occupy lower grades while older members have attained higher ranks. The supervisor-subordinate relationship is again raised because an ethical networking environment requires the efforts of all levels of an organization. The data for this hypothesis test is located in Appendix C.

Level of Command Consistencies. The final category tested was the question regarding at what *level of command* respondents worked. This category was divided into two groups. The first group is made up of those respondents at the Wing/Base, Group, and Directorate levels. These individuals are typically upper management policy makers. The other group consisted of responses from the Squadron, Flight, Division, Branch, and Section levels (including the *other* responses). This grouping was chosen to see how those in a management environment responded to the scenario questions as opposed to those who were at a lower-level—the actual workers and operators in non-policy making positions. .

The mean, standard deviations, and difference of means for each question were calculated for both groups. Once again, the null hypothesis tested was that the mean responses of the two groups would be the same (H_0: M_1=M_2) while the alternative hypothesis again stated that the responses would be different (H_A: M_1<M_2 or M_1>M_2). Similar to the hypothesis testing performed in the grade groupings, there was a difference in the number of respondents for each group. The Wing/Directorate level responses totaled 19 while the Squadron/Division level responses totaled 68. A p-value for each question was calculated. This statistic was again computed based on a .10 level of significance and the assumptions that both sampled populations had an approximately normal relative frequency distribution, the variances of the populations were equal, and the samples were randomly and independently selected from their respective populations.

The two values found to be significant in the groups are in Scenario 2 and Scenario 6. In Question d of Scenario 2 respondents were asked if Carol should alert the system administrator of the system she accessed regarding the ease at which their system was compromised. The mean at the upper management levels (Mean = 4.00) was in favor of alerting the compromised system administrator. However, the lower-level individuals had a lower mean (Mean = 3.61). This may be an indication about how respondents view their current environment. Several respondents wrote in on the survey next to this question remarks like: “Sure, if she wants to go to Leavenworth.” This may mean that the lower-level workers are aware of the issues but are more concerned with the punishment of the action instead of actually doing the right thing where networks are concerned. In Scenario 6 Question d stated that “Joanne’s use of the phone was entirely inappropriate, phones are reserved for official use only and should not be used for any kind of personal business.” Upper-level managers were more inclined to agree that Joanne’s use was inappropriate (Mean = 3.32) while lower-level employees were more lenient (Mean = 2.77). This may indicate a discrepancy in the views between the two groups because upper-level managers are more likely to have come from the ranks of the lower-level employees. These managers began their careers when organizations were more structured and less focused on an empowered work force. The emphasis on Quality Management in the last several years has loosened some of the restrictions placed on workers to enhance efficiency and morale. This is the atmosphere of the lower-level employees currently. Therefore, the responses from the lower-level group may indicate a better awareness of local policies and practices.

Thirty of the 32 p-values for this group were found to have no significant difference between the two groups. This consistency between the means indicates there is little difference in the responses between the different levels of command. This is a positive finding because it may indicate that all levels of the organization are applying similar guidance regarding behavior in the USAF’s networked *infosphere*. The data for this test is located at Appendix D.

V. Conclusions and Recommendations

Introduction

This study has addressed the "new species" of traditional ethical issues currently faced in the workplace today (Johnson, 94:10). The unique aspects of networking technology and the ethical issues encompassed by the new networked environment have been discussed in the preceding chapters. A review of the primary DoD and USAF publications dealing with computer and network usage found that the both the DoD and the USAF have acknowledged that a networked environment presents new situations about which ethical decisions must be made. Finally, a survey of USAF members has provided data indicating that members generally do not differ in their views regarding network capabilities. This chapter summarizes the study and provides a discussion of the conclusions drawn from the research questions presented in Chapter I.

Discussion

Although the use of computers and computer networks in the workplace provides a new area for ethical judgments, the study found a striking agreement on appropriate actions and behaviors. The first research question explored the differences between a networked environment and a traditional work environment. The second research question provided a USAF managerial focus on the issues encompassed by a networked environment. The final question, and the focus of the study, provided a user perspective on the issue of new ethical issues in the networked workplace.

Inconsistencies in the views expressed on the survey could indicate potential problems for the USAF in the area of appropriate, ethical usage of USAF resources.

The responses of USAF members participating in the survey administered as part of this study indicate that the members recognize this transformation of the traditional, familiar workplace of the past and are not continuing with business as usual. One of the most encouraging findings of the study is that there are very few significant differences in USAF member views regarding the features of a networked environment. A basic statistical analysis of three groupings of the respondents did not show any significant differences in their responses to the questions pertaining to each scenario presented.

Seven items were found to have a significant difference between the groups compared. One item concerned an issue of government property usage on a personal computer. In this instance, officer responses were found to be more inclined to disagree with the usage of government property in the home than enlisted responses. Another item addressed the illegal access of a private computer network. In this case, upper-level managers believed the perpetrator of the access notify the owner of the system to inform them of how easily their system was compromised. Lower-level employees did not believe as strongly as management that the individual should tell the compromised system's owner. Many responses included a write-in comment regarding the fact that she will be punished if authorities discover what she did. An additional difference between the groups was found to be in the area of privacy information control and access. The responses from the 31+ age group were more likely to disagree with gathering privacy information than the 18-30 year old group. This finding could indicate that some education is necessary regarding government responsibilities regarding private information.

The final four items found to have differences between the groups were located in Scenarios 4 and 6. In Scenario 4 the differences in the responses were found regarding the use of government resources during off-duty time and what constitutes appropriate usage when those resources are used. In both cases, the 31+ age group felt it was less appropriate for these actions while the 18-30 age group did not feel as strongly about the issue. The USAF and its managers need to ensure all employees are aware of the appropriate usage of government information resources.

In Scenario 6 the 2 issues found to have significant differences were those involving the performance of personal business over government phones and information networks. The 18-30 year group was more likely to agree there is nothing wrong with limited usage as long as it doesn't interfere with her job. The 31+ year group were more inclined to disagree with the performance of limited personal business. For the use of phones the upper-level responses were more likely to fall in a higher range than the lower-level responses. These findings indicate the possibility for conflict in the workplace if the differences are not addressed.

The Specific Research Objective

The objective of this study was to provide a preliminary understanding of what ethical issues are facing USAF members in the workplace today, and how members perceive these issues in terms of the ethical development of a networked work environment. This understanding was provided by identifying the issues USAF members currently face and by finding out how the USAF is dealing with these issues from a managerial level. Most importantly, the survey responses provide a preliminary understanding of how USAF members respond to scenarios that involve ethical issues in today's workplace.

Limitations of Current Study

This study presents the results of a survey of user beliefs about ethical issues as they apply in a networked environment. Limitations of this type of exploratory study include sample size, population representation, and the restrictive nature of survey questions. Of particular note is the issue of how representative the sample (WPAFB) is to the entire population of interest (USAF). This study examined only USAF members on one base. A broader variation of respondents from different bases could provide data more representative of the USAF as a whole.

Recommendations for Future Research

Replication of this study with varying study populations could help learn if the results can be generalized across the entire USAF. In addition, widespread downsizing of the military and outsourcing of activities to private contractors increase the base of authorized system users. A study including the civilian and contractor populations as well as the military population may provide a more comprehensive view on the actual status of ethical standards in the workplace. A long-term longitudinal study would also be beneficial because data could be tracked regarding how ethical views of networking are altered over time with the addition of new features to current technologies and the introduction of new technologies to the workplace.

A Final Word: Implications for USAF Managers

There is every indication that computers and networks will continue to expand their influence into the 21st century. The potential for the development of inappropriate ethical standards in the networked workplace is a very real threat to organizations. To ensure USAF assets, including its members, maintain the highest standards of integrity, ethical issues surrounding information networks must be addressed at every level. Organizational policies dealing with the ethical issues of networking requires involvement at all levels; users, technicians, managers, and others must cooperate to ensure the development of an ethical environment which will be supported by all members. The policies must be restrictive enough to effectively promote an ethical environment, yet flexible enough to enable workers to make some of their own decisions. Users need policies which let them feel like it is in their own best interest to comply (Jones, 1991:13). Just as in an effective security program, the strength of an organization's ethical policies is based largely on awareness and compliance by employees (Jones, 1991:66).

As technology continues to advance, additional issues and challenges will likely arise with ethical implications. Organizations must be proactive in meeting these challenges to maintain an ethical atmosphere in the work environment. In 1992 Ernest

Kallman stated, “dealing with unethical computer use requires the same management skill and attention as any other kind of organizational risk” (Kallman, 1992:69). He recommended that unethical computer use “must be considered as a risk to be planned for and managed just as are risks from physical disasters, precipitous government action, market forces, and the like” (Kallman, 1992:69). This study addressed the preliminary aspects of ethical computer usage in the USAF. Although an exploratory study of this scope cannot capture all the long-term ramifications of the revolutionary developments in computing, it can provide the preliminary understanding of how networking is currently affecting the USAF work environment.

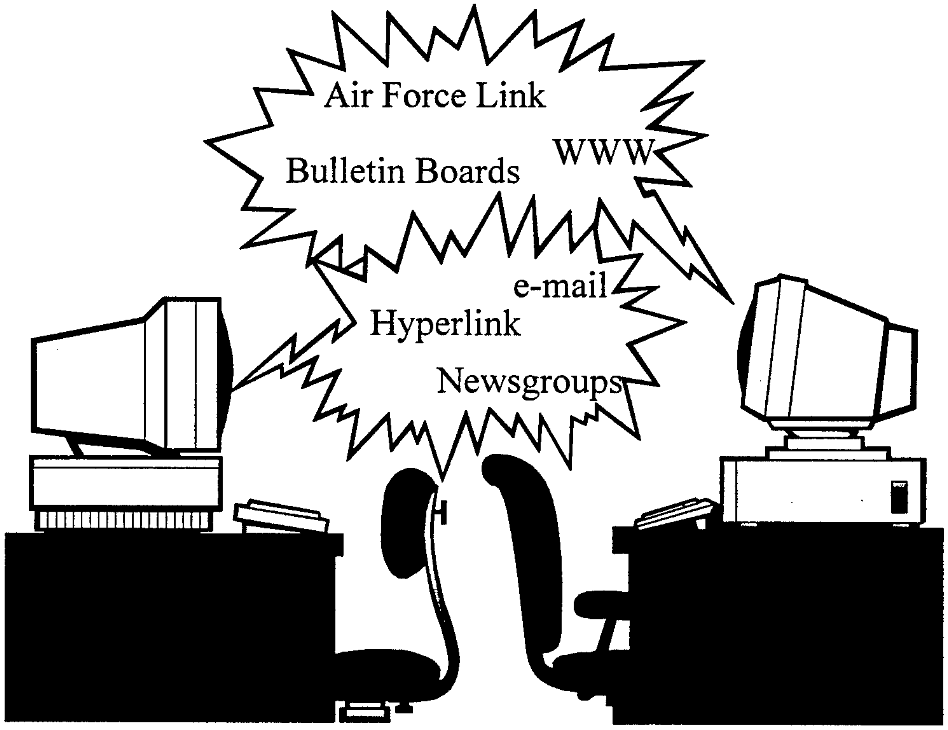
Appendix A: Survey

USAF SURVEY CONTROL: 98-12
Expiration Date: 30 Sep 98

AIR FORCE INSTITUTE OF TECHNOLOGY

USER PERCEPTIONS IN A NETWORKED ENVIRONMENT

USAF NETWORK USAGE SURVEY



Capt Kristen Sallberg
AFIT/LAA
Wright-Patterson AFB OH

USER PERCEPTIONS IN A NETWORKED ENVIRONMENT

INSTRUCTIONS:

This survey is designed to gather important information about the perceptions of USAF employees regarding performance in a networked environment. This data will be used to identify issues concerning computer ethics which apply to the USAF workplace. The survey consists of 16 general questions and 8 scenarios with 32 statements regarding ethical issues potentially applicable to usage of USAF data communications networks. Please answer the questions by filling in the blanks or circling your answer. All responses will be anonymous. Completing this survey should take no longer than 20 minutes. Please return, via base distribution within one week of receipt, to Captain Sallberg—AFIT/LAA. Thank You!

PART I: Background Demographics

1. What is your grade?

   a. E-1 to E-3
   b. E-4 to E-5
   c. E-6 or above
   d. 0-1 to 0-2
   e. 0-3 to 0-4
   f. 0-5 or above
   g. other_______

2. What is your age group?

   a. 18-25
   b. 26-30
   c. 31-35
   d. 36-40
   e. 41 or above

3. How long have you been employed by the United States Air Force?

   a. 1-5 years
   b. 6-10 years
   c. 11-15 years
   d. 16-20 years
   e. More than 20 years

4. How long have you been working in your present office?

   a. Less than one year
   b. 1-2 years
   c. More than 2 but less than 5 years
   d. More than 5 but less than 8 years
   e. More than 8 years

5. At what level of command is your office located?

   a. Wing/Base
   b. Group
   c. Squadron
   d. Flight
   e. Directorate
   f. Division
   g. Branch
   h. Section
   i. Other _________

6. Do you directly supervise employees? YES NO
   If yes, how many? _________

7. If you do not directly supervise employees are you considered a manager? YES NO (for example; Division Chiefs or Technical Directors may not officially rate any employees but are still involved in policy making)

8. Do you consider yourself a:

   a. computer user (one who uses computers in the office but does not design or program)

   b. computer professional (one who is able to program, design, or configure a computer or computer network)

PART II: Network Related Data

For the purposes of this survey, a network refers to any computer system by which a user can transmit and/or receive information (e-mail, internet access, World Wide Web pages, electronic bulletin boards).

9. Approximately how long has your office had access to a network?

a. Less than one year
b. 1-2 years
c. More than 2 but less than 5 years
d. More than 5 but less than 8 years
e. More than 8 years
f. My office does not have access to a network

10. What do you use your network access for? (Circle as many as apply, this list is not all-conclusive—feel free to indicate anything you use that is not on the list)

a. E-mail
b. Organizational bulletin board
c. Internet/World Wide Web access
d. Access to organizational documentation
e. Distribution of documentation
f. Other ___________________

11. In your present position, how often do you use your office network?

a. Do not use network
b. At least once a month
c. At least once a week
d. At least once a day
e. Several times each day
f. I log on upon arrival at work and work on the network throughout the day

12. Do you use the network to accomplish:

a. All of your work
b. A majority of your work
c. Some of your work
d. Very little of your work
e. None of my work

13. How would you rate the effectiveness of networking in enhancing your duty performance?

1-------2-------3-------4-------5-------6-------7-------8-------9-------10
not at all effective *somewhat effective* *extremely effective*

14. Has your organization provided you information or guidance regarding appropriate usage of organizational computer networks?

YES NO

15. Have you ever observed or experienced what you, as a user, consider to be inappropriate usage of computers or computer networks within the workplace?

YES NO

16. If question 15 was answered yes can you describe the experience(s)?

PART III. Sample Scenarios

The following scenarios are each stand-alone. No one scenario pertains to any other scenario. In each scenario the characters are identified by name only; they may be military members or civilian employees. Each scenario is fictional and has no tie to the United States Air Force. The scenarios have been developed solely as survey tools and are not meant to mirror any true situation.

Please rate your response to the statements following each scenario according to the scale provided directly beneath each scenario. Circle the number of your response (1, 2, 3, 4, or 5) provided to the left of each statement. Please rate each statement according to your initial reaction, which may not be consistent with what the published policies or instructions dictate. If you have any comments regarding the scenario there is a blank space following each set of statements. Continue on the back of the page if necessary.

1. Jack works at Any AFB. He has just been assigned a new engineering project. Success in this project could bring big benefits to the Air Force as well as a promotion for Jack. To complete this project a specific version of a popular off-the-shelf software package is required. This software is acquired and specially configured, at considerable expense, for Jack's organization. The software has been loaded on to the organization's network. Jack is so excited about the project that he begins to work nights at home. Since he is working on the project in his home, he logs into the network at work and downloads the software to his personal computer "just in case" he can't get a network connection when he needs it. He is also concerned that there might be a problem with the server at work and he wants to make sure he maintains a back-up copy of his data on his home computer as an extra precaution. He does not inform anyone in his computer department that he did this. His wife discovers the program on the computer and uses it for some of the freelance work she prepares for a private corporation.

|------------------------|-----------------------|-------------------------|----------------------|

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. It is okay that Jack downloaded the software; he had valid reasons.

1—2—3—4—5 b. Because Jack is working so many extra hours without compensation, he's allowed to download the software.

1—2—3—4—5 c. There is no problem with Jack's wife using the software as long as he is not using it.

1—2—3—4—5 d. Since the Air Force is going to benefit, it's okay if Jack uses the software on his home computer.

Additional Comments:

2. Susan and Carol work at Any AFB and have been friends for many years. Susan works in the security office and Carol is a budget specialist. Susan's seventeen-year-old son has been troubled since his parents divorced when he was eleven years old. He recently began charging things to her credit card then hiding the statements when they came in the mail. He has also forged several checks which has caused Susan to bounce a few checks for household utilities. Susan is concerned her credit rating is receiving some black marks which she is afraid may reflect on her upcoming security clearance update. She is very worried that she could lose her job due to her son's irresponsibility. One of Carol's hobbies is surfing the Internet to use the bulletin boards and chat rooms used by amateur hackers. Carol notices how upset Susan is when they have lunch one day and Susan details the whole story. When she gets back to her office Carol takes it upon herself to gain access to the credit bureau to see how bad the situation really is. Once she accesses the system she learns that things are not quite as bad as Susan thinks they are. Carol exits the accessed system without trying to make any changes to data. She gives Susan a call later that evening to let her know the "good news."

|-------------------------|------------------------|--------------------------|------------------------|

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Carol's actions would not be considered wrong.

1—2—3—4—5 b. As long as she did not change the system she gained access to, it's okay for Carol to "browse" the system's data.

1—2—3—4—5 c. If an employee of the bank where Susan's checks have been bouncing decides to access the same system Carol accessed to see what Susan's financial situation is, that would be an entirely appropriate action.

1—2—3—4—5 d. Carol should alert the system administrator of the system she accessed about how easily their system was compromised.

Additional Comments:

3. Bill is a senior level manager at Any AFB. He and Mary, an employee in the personnel department of the same organization, are just starting up a small computer consulting business to fill up their spare time. They came up with a great idea to expand the company and would like to offer the opportunity to some of the folks they work with in their organization. Since they know it would be improper to approach these individuals during duty hours at the base, Bill asks Mary to pull the home phone numbers, addresses, and home e-mail addresses of the people they want to contact to offer their opportunity from the organization's personnel database. They then use this information to mail some initial documentation to the people's homes and follow up with a call to the people on the weekend.

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Bill's request to Mary was perfectly legitimate.

1—2—3—4—5 b. There is no problem with Mary gathering the information off the network.

1—2—3—4—5 c. Since it was just general information, there is no problem with using the information off the network.

1—2—3—4—5 d. I would have no problem with someone from work providing my home phone number or address to someone who would be offering me a great opportunity for additional income and advancement.

Additional Comments:

4. Paul is a computer programmer at Any AFB. He began a small side business preparing folios surrounding new technology investments by gathering and consolidating information, primarily from the Internet. Since his Internet provider was difficult to use on the weekends because it was so busy, he would often go into the office on weekends to work on his folios. He was required to sign in and out at the front door and used his system user identification code to sign onto the machine. This information showed when he was in the building and how long he used the system; therefore, he was not trying to hide his actions.

|--------------------------|--------------------------|--------------------------|--------------------------|

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Paul should not have a business on the side.

1—2—3—4—5 b. Paul's use of the organization's computer was completely appropriate because it was not being used over the weekend and the resources would just be sitting idle.

1—2—3—4—5 c. Since he was gathering non-government information, there is no problem with using the network in this manner; it's all information in the public domain.

Additional Comments:

5. Cliff works in the data entry division at Any AFB. His organization has been going through many changes in the last year or so, reengineering their processes and transitioning over to new information technology. Cliff has been performing his particular job for ten years. His duties entailed inputting information into a DoD-wide database which was used to keep senior officials informed of the political climate of various countries. One day Cliff's boss came by about 1030 and told his section that the new upgrade to the database had finally been loaded after a two-year delay. For the data entry people, this upgrade changed a few of the input fields but little else. The input screens looked the same as the old input screens but several of the fields were swapped with each other. Since Cliff was so used to the old screens, he usually performed on "autopilot" and rarely needed to look at the screen. In addition, the change was so subtle that unless users closely examined the screen they would not be able to tell any changes had been made. Cliff was an early riser and had already spent over three hours inputting data into the database. In this time he had been able to input almost 100 documents. To find these documents and make the corrections would take hours and involve several different departments. Cliff thinks the batch of documents he input that morning was not particularly important. Since he also performed quality control for his area he knew no one would be checking up on his work. He makes the decision to leave the inaccurate information in the database and begin using the new screen with the next document. Cliff reasons to himself that because there are millions of records in this database, the last hundred or so shouldn't make much difference.

```
|------------------------|-----------------------|-------------------------|----------------------|
```

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Cliff was right to continue on without spending the government's time and money on such a minor error.

1—2—3—4—5 b. The system designers did a good job designing the system because there is a very small learning curve for Cliff's area.

1—2—3—4—5 c. The computer division did not need to provide the system users with a timeframe for the system upgrade; they are responsible for the entire network and can change the configuration whenever they want to.

1—2—3—4—5 d. Cliff's actions are entirely appropriate because it was his boss' fault for not getting to his people sooner to warn them about the immediate change.

Additional Comments:

6. Joanne is an employee at Any AFB. She is a good employee and always gets her work done on time if not before. Sometimes she has some "dead-time" when she has finished her previous work and is waiting for her next assignment. During this time she often browses the Internet to keep herself busy. One of the primary places she accesses gives her the most current stock information so she can check on her portfolio. She sometimes needs to phone her broker on occasion when she observes something on the Internet which may pertain to her. She also accesses government sites which keep her up to date with her current job.

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Joanne's use of her "dead-time" is entirely appropriate; it is much more productive than going to the cafeteria and sitting over coffee.

1—2—3—4—5 b. There is nothing wrong with Joanne performing limited personal business over the organization's network as long as it does not interfere with her job.

1—2—3—4—5 c. Joanne should let her boss know when she has "dead-time" so he can make a decision about what she should do with her time.

1—2—3—4—5 d. Joanne's use of the phone was entirely inappropriate; phones are reserved for official use only and should not be used for any kind of personal business.

Additional Comments:

7. John's supervisor, Alan, is worried that John has forwarded some information to the Commander regarding a disagreement over a funding decision. Alan used to work in the computer division and still has friends there. Alan calls the system administrator in his old office and asks him to use his system privileges to scan through John's e-mail traffic to see if there is any correspondence between John and the Command Section. Although none is found, the administrator tells Alan that he did find several messages between John and a supervisor in another division regarding an upcoming opening John was interested in. Based on the information from the administrator, Alan does not consider John for a promotion in his area because he discovered John was thinking of leaving.

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Alan is perfectly within his right as a supervisor to acquire the information he received in any manner he deems appropriate.

1—2—3—4—5 b. There is nothing wrong with the system administrator auditing John's files; it's part of the system administrator's job.

1—2—3—4—5 c. John's use of the system to send messages back and forth regarding a new job is not appropriate.

1—2—3—4—5 d. The system administrator had every right to provide Alan information outside the realm in which Alan was asking.

1—2—3—4—5 e. John has a right to file a complaint against Alan and the administrator for accessing his personal files.

Additional Comments:

8. Robin is an administrator in the Commander's office. She is an excellent employee and consistently receives the highest ratings. The Vice-Commander has asked Robin to show his new secretary, Karen, how to use the network to support Command Section processes. Karen has very little experience with computers and no experience at all with network usage. She has never used an e-mail account nor has she ever accessed information posted on the network. While Robin was showing Karen how to use the e-mail system she accessed her own account to demonstrate how to save files, use attachments, and set up consolidated work-group aliases. During this demonstration Robin received a message in her e-mail in-box. She used the opportunity to show Karen how to receive, read attachments, and reply to messages. The incoming e-mail was from Robin's daughter at a college a few hours away. She was letting Robin know that it was time for her to send her tuition check to the college. Her daughter also included some anecdotes about her life in the dorm and provided an update on her classes. Robin quickly replied to the message with a quick "the check is in the mail" and included "keep up the good work, talk to you soon, Love you! Mom". Once Robin had sent the reply, while explaining the procedure to Karen, they continued on with Robin's demonstration. Later that afternoon Karen sent an anonymous note to the Fraud, Waste, and Abuse Office reporting Robin for unauthorized use of a government resource.

1	2	3	4	5
Strongly Disagree	Disagree	Neither Agree nor Disagree	Agree	Strongly Agree

1—2—3—4—5 a. Karen was acting appropriately in reporting Robin.

1—2—3—4—5 b. Robin receiving the message from her daughter was not a problem, but Robin replying to the message over the network was inappropriate.

1—2—3—4—5 c. It was Karen's responsibility, as a government employee, to report Robin.

1—2—3—4—5 d. Robin should be disciplined for using the network the way she did.

Additional Comments:

THANK YOU for participating in this survey!

Upon completion please place the survey in the envelope provided and place in the base distribution system for return to Capt Sallberg, AFIT/LAA.

Your inputs are greatly appreciated and will be beneficial for understanding how military members view computer networks in the work environment of the USAF. All information provided will be used solely for consolidation and reporting as part of the entire study; individual responses will remain anonymous and be secured properly. Additionally, data collected can be requested IAW the Freedom of Information Act. If you have any questions or comments please reply to Capt Kristen Sallberg, AFIT/LAA, Wright-Patterson AFB, OH DSN 785-7777 x2155, ksallber@afit.af.mil.

Appendix B: Difference between the Means Responses for Grade Groups

Difference between Officer (M_1) Responses and Enlisted Responses (M_2)
($n_1 = 61$, $n_2 = 28$)

Scenario Question	M_1	M_2	SD_1	SD_2	M_1-M_2	z-stat	p-value
S1a	2.89	3.00	1.47	1.39	0.115	0.258	0.242
S1b	1.85	2.50	1.28	1.29	0.648	1.767	0.127
S1c	1.44	1.36	.81	0.87	-0.085	-0.533	0.103
S1d	2.82	3.04	1.43	1.37	0.216	0.502	-0.002
S2a	2.03	1.93	1.17	1.25	-0.104	-0.315	0.815
S2b	1.69	1.71	0.94	1.15	0.026	0.097	0.403
S2c	2.89	3.11	1.27	1.29	0.222	0.611	-0.111
S2d	3.55	4.07	1.01	0.98	0.522	2.415	0.192
S3a	1.49	1.64	0.60	1.03	0.151	0.767	-0.267
S3b	1.61	1.64	0.82	1.03	0.036	0.173	0.327
S3c	1.61	1.43	0.88	0.74	-0.178	-1.271	0.771
S3d	1.52	1.50	0.81	0.69	-0.025	-0.204	0.704
S4a	1.48	1.61	0.70	0.88	0.132	0.864	-0.364
S4b	1.71	1.50	0.93	0.64	-0.213	-1.610	0.211
S4c	1.73	1.68	0.95	1.06	-0.051	-0.219	0.719
S5a	1.54	1.64	0.85	0.78	0.102	0.712	-0.212
S5b	2.39	2.96	1.13	0.69	0.571	3.120	0.620
S5c	1.67	2.18	0.68	0.86	0.506	3.435	0.293
S5d	1.72	2.00	0.92	0.77	0.279	1.846	0.346
S6a	3.04	2.78	1.18	1.31	-0.263	-0.735	0.123
S6b	3.01	2.50	1.27	1.23	-0.508	-1.478	0.198
S6c	3.61	3.57	0.88	1.14	-0.035	-0.138	0.638
S6d	2.68	3.39	1.11	1.17	0.713	2.438	0.194
S7a	1.41	1.57	0.64	0.84	0.162	1.175	-0.675
S7b	2.21	2.21	1.18	1.20	0.001	0.004	0.496
S7c	1.70	2.57	0.76	1.23	0.867	3.038	0.253
S7d	1.49	1.68	0.70	0.77	0.187	1.496	-0.996
S7e	4.13	3.79	0.94	1.23	-0.345	-1.165	0.665
S8a	2.00	2.39	1.02	1.13	0.393	1.467	-0.967
S8b	1.98	2.68	0.88	1.12	0.695	2.775	0.227
S8c	2.26	2.71	1.09	1.24	0.452	1.415	-0.915
S8d	1.87	2.25	0.92	1.21	0.381	1.334	-0.834

Appendix C: Difference between the Means Responses for Different Age Groups

Difference between Responses by Age Groups
(n_1=41; n_2=48)

Scenario Question	M_1	M_2	SD_1	SD_2	M_1-M_2	z-stat	p value
S1a	3.29	2.60	1.35	1.45	0.689	0.69	-0.19
S1b	2.17	1.96	1.34	1.29	0.212	0.21	0.29
S1c	1.49	1.35	0.68	0.93	0.134	0.13	0.37
S1d	3.27	2.56	1.20	1.50	0.706	0.71	-0.21
S2a	2.27	1.77	1.36	0.97	0.497	0.06	0.44
S2b	1.78	1.63	1.06	0.96	0.155	0.16	0.34
S2c	3.12	2.81	1.27	1.27	0.309	0.31	0.19
S2d	3.71	3.71	1.03	1.03	-0.001	0.00	0.50
S3a	1.73	1.38	0.90	0.57	0.357	0.36	0.14
S3b	1.90	1.38	1.09	0.57	0.527	0.53	-0.03
S3c	1.76	1.38	1.76	0.64	0.381	0.38	0.12
S3d	1.54	1.50	1.54	0.71	0.037	0.04	0.46
S4a	1.44	1.58	1.44	0.79	-0.144	-0.14	0.64
S4b	1.94	1.40	1.94	0.76	0.543	0.54	-0.04
S4c	2.01	1.46	2.01	0.94	0.554	0.55	-0.05
S5a	1.71	1.46	1.71	0.82	0.249	0.25	0.25
S5b	2.78	2.40	2.78	1.03	0.385	0.38	0.12
S5c	1.98	1.71	1.98	0.68	0.267	0.27	0.23
S5d	1.90	1.73	1.90	0.96	0.173	0.17	0.33
S6a	3.34	2.65	3.34	1.30	0.692	0.69	-0.19
S6b	3.09	2.65	3.09	1.39	0.440	0.44	0.06
S6c	3.49	3.69	3.49	0.97	-0.200	-0.20	0.70
S6d	3.01	2.81	3.01	1.25	0.200	0.20	0.30
S7a	1.49	1.44	1.49	0.71	0.050	0.05	0.45
S7b	2.59	1.90	2.59	1.12	0.690	0.69	-0.19
S7c	2.00	1.96	2.00	1.07	0.042	0.04	0.46
S7d	1.61	1.50	1.61	0.71	0.110	0.11	0.39
S7e	4.02	4.02	4.02	1.16	0.004	0.00	0.50
S8a	2.12	2.13	2.12	1.02	-0.003	0.00	0.50
S8b	2.10	2.29	2.10	1.03	-0.194	-0.19	0.69
S8c	2.44	2.38	2.44	1.12	0.064	0.06	0.44
S8d	2.00	1.98	2.00	1.10	0.021	0.02	0.48

Appendix D: Difference between Responses for Different Levels of Command

Difference between Responses for Different Levels of Command
(n_1=19; n_1=68)

Scenario Question	M_1	M_2	SD_1	SD_2	M_1-M_2	z-stat	p-value
S1a	2.95	2.91	1.39	1.47	0.036	0.072	0.428
S1b	2.42	1.97	1.39	1.29	0.450	0.972	-0.472
S1c	1.63	1.35	1.07	0.75	0.279	0.191	-0.591
S1d	2.95	2.87	1.43	1.42	0.080	0.157	0.343
S2a	2.00	2.01	1.41	1.14	-0.015	-0.032	0.532
S2b	1.79	1.68	1.27	0.94	0.113	0.308	0.192
S2c	2.63	3.04	1.30	1.26	-0.413	-0.997	0.497
S2d	4.00	3.61	1.00	1.02	0.390	0.555	0.055
S3a	1.53	1.56	0.70	0.78	-0.033	-0.254	0.754
S3b	1.63	1.63	0.76	0.93	-0.001	-0.005	0.505
S3c	1.63	1.54	1.012	0.80	0.087	0.372	0.128
S3d	1.68	1.49	1.057	0.68	0.199	0.799	-0.299
S4a	1.84	1.43	1.068	0.63	0.416	0.647	-0.147
S4b	1.63	1.67	0.96	0.84	-0.038	-0.174	0.674
S4c	1.68	1.74	1.00	0.98	-0.058	-0.236	0.736
S5a	1.89	1.50	1.05	0.74	0.395	0.592	-0.920
S5b	2.47	2.62	0.84	1.11	-0.144	-0.678	0.178
S5c	1.84	1.82	0.60	0.83	0.019	0.164	0.336
S5d	1.79	1.82	0.71	0.93	-0.034	-0.225	0.725
S6a	3.00	2.99	1.37	1.17	0.007	0.016	0.484
S6b	2.53	2.95	1.26	1.26	-0.422	-0.066	0.566
S6c	4.00	3.49	0.88	0.97	0.515	0.536	-0.236
S6d	3.32	2.77	1.20	1.12	0.544	0.556	-0.056
S7a	1.58	1.40	0.69	0.65	0.182	0.571	-0.171
S7b	2.21	2.21	1.23	1.17	0.005	0.013	0.487
S7c	2.16	1.91	1.17	0.97	0.246	0.776	-0.276
S7d	1.58	1.54	0.77	0.72	0.035	0.244	0.256
S7e	3.89	4.04	1.20	1.01	-0.149	-0.446	0.946
S8a	2.05	2.15	0.97	1.10	-0.094	-0.378	0.878
S8b	2.16	2.24	1.02	1.02	-0.077	-0.302	0.802
S8c	2.53	2.38	1.22	1.15	0.144	0.401	0.099
S8d	2.11	1.97	1.20	0.99	0.135	0.405	0.095

Bibliography

Abshire, Gary M. "The Ethical Insensitivity of Computer Specialists and What You Can Do About It," Computers and Society, 12:, 10-11 (Winter 1982).

Air Force Issues Book. "Obligations to the Taxpayer." WWWeb, http://www.af.mil/lib/afissues/1995/sec6.html.

Air Force News Service. "Government E-mail Subject to Abuse," Air Force News Service article, 2 pages. WWWeb, http://www.af.mil/news/Jan1997/n19970115_970051.html. 15 January 1997.

Air Force News Service. "Officer Dismissed for Computer Porn." Air Force News Service article, 1 page. WWWeb, http://www.af.mil/cgi-bin/waisgate. 9 May 1997.

Air Force News Service. "Web Surfing Officer Nets Nine Month Confinement." Air Force News Service article, 2 pages. WWWeb, http://www.af.mil/cgi-bin/waisgate. 11 February 1997.

Baase, Sara. A Gift of Fire. Upper Saddle River NJ: Prentice Hall Inc., 1997.

Barbour, Ian G. Ethics in an Age of Technology. San Francisco CA: Harper Collins, 1993.

Barlow, John P. "Coming into the Country," Communications of the ACM, 34: 19-21 (March 1991).

Basso, Joseph. "How Public Relations Professionals are Managing the Potential for Sabotage, Rumors, and Misinformation Disseminated Via the Internet by Computer Hackers," IEEE Transactions on Professional Communication, 40: 28-33 (March 1997).

Bordia, Prashant. "Face-to-Face Versus Computer Mediated Communication: A Synthesis of the Experimental Literature," The Journal of Business Communication, 34: 99-120 (January 1997).

Boudourides, Moses A. "Social and Psychological Effects in Computer-Mediated Communication," Contributed Paper at the 2nd Workshop/Conference Network '95. 10 pages. WWWeb, http://192.108.114.10/~mboudour/mab/csi.html. 12 October 1995.

Brewin, Bob. "Computer Crime; Soldier Faces Courts-martial in Espionage Case," Federal Computer Week: 6 (26 August 1996).

Burnett, Kay L. "Ethics and IT: Is the Human Factors Approach an Ethical Way of Designing and Implementing Information Technology?" in Social and Ethical Effects of the Computer Revolution. Ed. Joseph Migga Kizza. Jefferson NC: McFarland & Company, Inc., Publishers, 1996.

Clement, Andrew. "Computing at Work: Empowering Action By 'Low-level Users'," Communications of the Association for Computing Machinery, 37: 53-63 (January 1994).

Compart, Andrew. "Master Sergeant is Sent to Jail in E-mail Case," Air Force Times, 57: 6 (10 June 1996).

Cooper, Donald R. and C. William Emory. Business Research Methods (Fifth Edition). Chicago IL: Richard D. Irwin, Inc., 1995.

Culnan, Mary J. "'How Did They Get My Name?' An Exploratory Investigation of Consumer Attitudes Toward Secondary Information Use," MIS Quarterly, 17: 341-363 (September 1993).

Dejoie, Roy, and others. Ethical Issues in Information Systems. Boston MA: Boyd and Fraser Publishing Company, 1991.

Department of the Air Force. Communications and Information: Information Protection. AFPD 33-2. Washington: HQ USAF, 1 December 1996.

Department of the Air Force. Electronic Mail (e-mail) Management and Use. AFI 33-119. Washington: HQ USAF, 1 March 1997.

Department of the Air Force. Transmission of Information via the Internet. AFI 33-129. Washington: HQ USAF, 1 January 1997.

Department of the Air Force. United States Air Force Core Values. Washington: HQ USAF, 1 January 1997.

Department of Defense. Joint Ethics Regulation. DoD 5500.7-R. Washington: OASD, 25 March 1996.

Ermann, M. David, and others. Computers, Ethics, and Society (Second Edition). New York: Oxford University Press, 1997.

Fitzgerald, Jerry and Alan Dennis. Business Data Communications & Networking (Fifth Edition). New York: John Wiley & Sons, 1996.

Fogelman, Ronald R., Chief of Staff, United States Air Force. "The Fifth Dimension of Warfare." Remarks delivered to the Armed Forces Communications and Electronics Association. Washington DC: 25 April 1995.

Forester, Tom and Perry Morrison. Computer Ethics: Cautionary Tales and Ethical Dilemmas in Computing (Second Edition). Cambridge MA: The MIT Press, 1995.

Geison, Gordon G. The New Logic of Hypertext: Electronic Documents, Literary Theory, and Air Force Publications. MS thesis, AFIT/GIR/LAC/96D-2. School of Logistics and Acquisition Management, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, December 1996 (AD-A319630).

Hamblen, Diane. "Careful! The NCIS Cybersleuths are Watching!" Chips. WWWeb, http://www.norfolk.navy.mil/chips/archives/96_jul/file1.html. July 1996.

Harrington, Susan. "The Effect of Codes of Ethics and Personal Denial of Responsibility on Computer Abuse Judgments and Intentions," MIS Quarterly, 20: 257-278 (September 1996).

Harrington Susan J. and Rebecca L. McCollum. "Lessons from Corporate America Applied to Training in Computer Ethics," Computers and Society, 20: 167-173 (October 1990).

Henry, John W. and Margaret Anne Pierce. "Computer Ethics: A Model of the Influences on the Individual's Ethical Decision Making," Computer Personnel, 15: 21-27 (October 1994).

HQ USAF. "Air Force Electronic Bulletin Boards and Internet World Wide Web Home Pages." Electronic Message. 111600Z, 18 March 1997.

Huff, Chuck. "Unintentional Power in the Design of Computer Systems," Computers and Society, 26: 6-9 (December 1996).

Johnson, Deborah G. Computer Ethics (Second Edition). Englewood Cliffs NJ: Prentice-Hall Inc., 1994.

Johnson, Deborah G. "Ethics Online," Communications of the ACM, 40: 60-65 (January 1997).

Jones, Francis B. Human Factors in Network Security. MS thesis, United States Navy Naval Postgraduate School (NPS), Monterey CA, March 1991 (AD-A243110).

Kallman, Ernest A. "Developing a Code for Ethical Computer Use," Journal of Systems Software, 17: 69-74 (1992).

Kizza, Joseph M. Social and Ethical Effects of the Computer Revolution. Jefferson NC: McFarland and Company, Inc., 1996.

Kling, Rob. Computerization and Controversy: Value Conflicts and Social Choices (Second Edition). New York: Academic Press, Inc., 1996.

Ladd, John. "Ethics and the Computer World: A New Challenge for Philosophers," Computers and Society, 27: 8-13 (September 1997).

Langford, Duncan. "Ethics and the Internet: Appropriate Behavior in Electronic Communication," Ethics and Behavior, 6: 91-106 (Spring 1996).

Laudon, Kenneth C. "Ethical Concepts and Information Technology," Communications of the ACM, 38: 33-39 (December 1995).

Lea, Martin and Russell Spears. "Computer-Mediated Communication, Deindividuation and Group Decision-Making," International Journal of Man-Machine Studies, 34: 283-301 (1991).

Linowes, David F. "Your Personal Information Has Gone Public," in Computerization and Controversy; Value Conflicts and Social Choices (Second Edition). Ed. Rob Kling. New York: Academic Press, 1996.

Loch, Karen D. and Sue Conger. "Evaluating Ethical Decision Making and Computer Use," Communications of the ACM, 39: 74-83 (July 1996).

Lozo, Christopher. "Computer Expert Gets Hooked on Child Pornography via Internet; Courts-Martial Results in Airman Losing More Than Just His Career," Command Post: 6 (8 November 1996).

Mason, Richard O. "Four Ethical Issues of the Information Age," MIS Quarterly, 10: 5-12 (March 1986).

McClave, James T. and P. George Benson. Statistics for Business and Economics (Sixth Edition). Englewood Cliffs NJ:Prentice Hall Inc., 1994.

Moor, James H. "Towards a Theory of Privacy in the Information Age," Computers and Society, 27: 27-32 (September 1997).

Nelson, Jeffrey E. The Status of Computer Ethics Instruction at Air Force Education and Training Institutions. MS Thesis, AFIT/GIR/LSR/88D-9. School of Systems and Logistics, Air Force Institute of Technology (AU), Wright-Patterson AFB OH, December 1988 (AD-A205410).

Neumann, Peter G. Computer Related Risks. New York: Addison-Wesley Publishing Company, 1995.

Nissenbaum, Helen. "Computing and Accountability," Communications of the ACM, 37: 73-80 (January 1994).

Paige, Emmett Jr., Office of the Assistant Secretary of Defense. Memorandum, Use of DoD Information and Telecommunications Systems. The Pentagon, 20 October 1997.

Paradice, David B. "Ethical Attitudes of Entry-Level MIS Personnel," Information and Management, 18: 143-151 (1990).

Paradice, David B. and Roy M. Dejoie. "The Ethical Decision-Making Processes of Information Systems Workers," Journal of Business Ethics, 10: 1-21 (1991).

Pierce, Margaret Anne and John W. Henry. "Computer Ethics: The Role of Personal, Informal, and Formal Codes," Journal of Business Ethics, 15: 425-437 (December 1996).

Resnik, David. "Ethics in Cybersociety," Computers and Society, 26: 23-24 (December 1996).

Resnik, David. "The Ethics of Cyber Relationships," Computers and Society, 26: 16-19 (March 1996).

Rose, Lance. Netlaw: Your Rights in the Online World. New York: McGraw-Hill Book Company, 1995.

Rosenberg, Richard S. The Social Impact of Computers (Second Edition). New York: Academic Press, Inc., 1997.

Rubin, Richard. "Moral Distancing and the Use of Information Technologies: The Seven Temptations," in Social and Ethical Effects of the Computer Revolution. Ed. Joseph Migga Kizza. Jefferson NC: McFarland & Company, Inc., Publishers, 1996.

Schwartau, Winn. Information Warfare. New York: Thunder's Mouth Press, 1996.

Simons, John. "Don't Chat, Don't Tell? Navy Case Tests Privacy Limits," The Wall Street Journal, 14 January 1998, sec. B:1.

Sipior, Janice C. and Burke T. Ward, "The Ethical and Legal Quandary of Email Privacy," Communications of the ACM, 38: 48-54 (December 1995).

Smith, H. Jeff, and others. “Information Privacy: Measuring Individuals’ Concerns About Organizational Practices,” MIS Quarterly, 21: 167-196 (June 1996).

Spinello, Richard. Ethical Aspects of Information Technology. Englewood Cliffs NJ: Prentice-Hall, 1995.

Straub, Detmar W. and William D. Nance. “Discovering and Disciplining Computer Abuse in Organizations: A Field Study,” MIS Quarterly, 14: 45-60 (March 1990).

Weckert, John and Douglas Adeney. Computer and Information Ethics. Westport CT: Greenwood Press, 1997.

Weiland, Janet. “Introducing Ethics into the Computer World,” Freedom Magazine. n. pag. WWWeb, http://www.fredommag.org/english/vol2704/ethics.html. June 1997.

Weisband, Suzanne P. and Bruce A. Reinig. “Managing User Perceptions of Email Privacy,” Communications of the ACM, 38: 40-47 (December 1995).

Vita

Captain Kristen Gray Sallberg was born in Boston, Massachusetts, on 30 November 1966. She graduated from Natick High School in 1984, and from Case Western Reserve University, Cleveland, Ohio, in 1988, earning a double major in Political Science and History. Captain Sallberg was commissioned on June 5, 1991 after graduating from Officer Training School, Lackland Air Force Base, Texas. Her first assignment was as Section Commander for the 91st Missile Security Squadron of the 91st Missile Wing at Minot Air Force Base, North Dakota. In October 1992, Captain Sallberg was transferred to the National Air Intelligence Center (NAIC) at Wright-Patterson Air Force Base, Ohio, where she served as an Executive Support Officer for the Literature Exploitation Division and Branch Chief for the Technical Services Branch (Flight Library 2830). Captain Sallberg entered the Graduate School of Logistics and Acquisition Management in May 1996.

Captain Sallberg married Captain Scott Sallberg, originally of Spring Lake Park, Minnesota, in April 1992. They have two daughters, Elisabeth Eileen and Melissa Rose. Her next assignment will be to the Air Education and Training Command at Randolph Air Force Base, Texas.

Permanent Address: 15901 Pecan Pass
San Antonio, Texas 78247

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of the collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503

1. AGENCY USE ONLY (Leave blank)	**2. REPORT DATE** December 1997	**3. REPORT TYPE AND DATES COVERED** Master's Thesis

4. TITLE AND SUBTITLE
ETHICAL ISSUES IN A NETWORKED ENVIRONMENT

5. FUNDING NUMBERS

6. AUTHOR(S)
Kristen G. Sallberg, Captain, USAF

7. PERFORMING ORGANIZATION NAMES(S) AND ADDRESS(S)

Air Force Institute of Technology
2750 P Street
WPAFB OH 45433-7765

8. PERFORMING ORGANIZATION REPORT NUMBER

AFIT/GIR/LAS/97D-11

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

N/A

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 Words)*

The research objective was to provide a preliminary understanding of how USAF computer users perceive the ethical considerations of computer networks and how the USAF is addressing ethical issues of networked environments. A survey was undertaken to explore questions of ethics in the use of information networks. The literature review explored issues of ethics in the private sector and USAF guidance regarding use of official government resources. The sample population consisted of military members stationed at Wright-Patterson Air Force Base Ohio. The responses regarding certain attitudes about behaviors and actions in a networked environment were consistent overall. A significant difference was observed between seven responses that addressed the issues of information privacy, unauthorized access, use of government software in the home, and personal use of government networks. Regardless of grade, age or level of command, respondents generally responded in a similar manner to different situations. The findings suggest that USAF members are aware of ethical considerations in networked environments. The results also indicate USAF management is attuned with the professional community pertaining to the guidance provided to USAF members.

14. SUBJECT TERMS
Computer Ethics, Misuse, Abuse, Ethics, Networking, Accountability, Privacy, Property,

15. NUMBER OF PAGES
144

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	**18. SECURITY CLASSIFICATION OF THIS PAGE** UNCLASSIFIED	**19. SECURITY CLASSIFICATION OF ABSTRACT** UNCLASSIFIED	**20. LIMITATION OF ABSTRACT** UL

AFIT Control Number AFIT/GIR/LAS/97D-11

AFIT RESEARCH ASSESSMENT

The purpose of this questionnaire is to determine the potential for current and future applications of AFIT thesis research. **Please return completed questionnaire** to: AIR FORCE INSTITUTE OF TECHNOLOGY/LAC, 2950 P STREET, WRIGHT-PATTERSON AFB OH 45433-7765. Your response is **important.** Thank you.

1. Did this research contribute to a current research project? a. Yes b. No

2. Do you believe this research topic is significant enough that it would have been researched (or contracted) by your organization or another agency if AFIT had not researched it?
a. Yes b. No

3. **Please estimate** what this research would have cost in terms of manpower and dollars if it had been accomplished under contract or if it had been done in-house.

Man Years__________ $__________

4. Whether or not you were able to establish an equivalent value for this research (in Question 3), what is your estimate of its significance?

a. Highly Significant b. Significant c. Slightly Significant d. Of No Significance

5. Comments (Please feel free to use a separate sheet for more detailed answers and include it with this form):

____
Name and Grade

____
Organization

____
Position or Title

____
Address